arXiv:1211.3566v1 [math.CO] 15 Nov 2012

Free partially commutative groups, cohomology, and paths and circuits in directed graphs on surfaces

Alexander Schrijver[1]

Abstract. We show that for each fixed k, the problem of finding k pairwise vertex-disjoint directed paths between given source-sink pairs in a planar directed graph is solvable in polynomial time. In fact, it suffices to fix the number of faces needed to cover all sources and sinks. Moreover, the method can be extended to any fixed compact orientable surface (instead of the plane) and to rooted trees (instead of paths).

Our approach is algebraic and is based on cohomology over graph (nonabelian) groups. More precisely, let $D = (V, A)$ be a directed graph and let $(G, \cdot)$ be a group. Call two function $\phi, \psi : A \to G$ *cohomologous* if there exists a function $p : V \to G$ such that $p(u) \cdot \phi(a) \cdot p(w)^{-1} = \psi(a)$ for each arc $a = (u, w)$. Now given a function $\phi : A \to G$ we want to find a function ψ cohomologous to ϕ such that each $\psi(a)$ belongs to a prescribed subset $H(a)$ of G. We give a polynomial-time algorithm for this problem in case G is a graph group and each $H(a)$ is closed (i.e., if word xyz belongs to $H(a)$ then also word y belongs to $H(a)$).

The method also implies that such a ψ exists, if and only if for each $s \in V$ and each pair P, Q of (undirected) $s{-}s$ paths there exists an $x \in G$ such that $x \cdot \phi(P) \cdot x^{-1} \in H(P)$ and $x \cdot \phi(Q) \cdot x^{-1} \in H(P)$. (Here $\phi(P)$ is the product of the $\phi(a)$ over the arcs in P. Similarly, $H(P)$ is the (group subset) product of the $H(a)$.)

1. Introduction

In this paper we show that the following problem, the k *disjoint paths problem for directed planar graphs*, is solvable in polynomial time, for any fixed k:

(1) given: a planar directed graph $D = (V, E)$ and k pairs $(r_1, s_1), \ldots, (r_k, s_k)$ of vertices of D;
find: k pairwise vertex-disjoint directed paths $P_1, \ldots, P_k$ in D, where P_i runs from r_i to s_i $(i = 1, \ldots, k)$.

The problem is NP-complete if we do not fix k (even in the undirected case; Lynch [6]). Moreover, it is NP-complete for $k = 2$ if we delete the planarity condition (Fortune, Hopcroft, and Wyllie [5]). This is in contrast to the undirected case (for those believing NP≠P), where Robertson and Seymour [10] showed that, for any fixed k, the k disjoint paths problem is polynomial-time solvable for any graph (not necessarily planar).

Our algorithm is a 'brute force' polynomial-time algorithm. We did not aim at obtaining the best possible running time bound, as we presume that there are much faster (but possibly more complicated) methods for (1) than the one we describe in this paper. In fact, recently Reed, Robertson, Schrijver, and Seymour [9] showed that for undirected planar graphs the

[1] CWI and University of Amsterdam. Mailing address: CWI, Science Park 123, 1098 XG Amsterdam, The Netherlands. Email: lex@cwi.nl.

k disjoint paths problem can be solved in *linear* time, for any fixed k. This algorithm makes use of methods from Robertson and Seymour's theory of graph minors. A similar algorithm for directed planar graphs might exist, but probably would require extending parts of graph minors theory to the directed case.

Our method is based on cohomology over free (nonabelian) groups. For the k disjoint paths problem we use free groups with k generators. Cohomology is in a sense dual to homology, and can be defined in any directed graph, also if it is not embedded on a surface. We apply cohomology to an *extension* of the planar graph dual of D—just using homology to D itself seems not powerful enough.

This approach allows application of the algorithm where the embedding of the graph in the plane is given in an implicit way, viz. by a list of the cycles that bound the faces of the graph.

It also allows a more general application than (1). It is not necessary to fix the number k of pairs (r_i, s_i) but it suffices to fix the number p of faces of D such that each of $r_1, s_1, \ldots, r_k, s_k$ is incident with at least one of these faces. The planarity condition can be relaxed to being embeddable in some fixed compact orientable surface. (A compact orientable surface is any space obtained from the sphere by adding a finite number of 'handles'.) We can restrict for each arc a the connections that can be made over a. Moreover, the method extends to finding rooted trees instead of directed paths.

That is, for any fixed compact orientable surface S and any fixed p we give a polynomial-time algorithm for the following problem:

(2) given: a directed graph $D = (V, A)$ embedded on S, subsets $A_1, \ldots, A_k$ of A, pairs $(r_1, S_1), \ldots, (r_k, S_k)$, where $r_i \in V$ and $S_i \subseteq V$ $(i = 1, \ldots, k)$, such that there exist at most p faces such that each vertex in $\{r_1, \ldots, r_k\} \cup S_1 \cup \cdots \cup S_k$ is incident with at least one of these faces;
find: k pairwise vertex-disjoint rooted trees $T_1, \ldots, T_k$, where T_i is rooted in r_i, covers S_i and contains arcs only in A_i $(i = 1, \ldots, k)$.

There are several other variants of this problem where the methods below are applicable. We did however not see if our methods extend to compact *non*orientable surfaces.

2. Directed graphs and surfaces

We give some notation and terminology on directed graphs and surfaces. Directed graphs may have loops and parallel arcs. Nevertheless we sometimes write $a = (u, w)$, meaning that a is an arc from u to w. For each arc a from u to w, we define a^{-1} as the reverse arc from w to u. (This need not be an arc of D again.)

An (*undirected*) *path* is a word

(3) $$P = a_1 a_2 \cdots a_m,$$

where $a_i = a$ or $a_i = a^{-1}$ for some arc a $(i = 1, \ldots, m)$, such that the head of a_i is equal to the tail of a_i $(i = 1, \ldots, m-1)$. We allow $a_{i+1} = a_i^{-1}$ in (3). Moreover we allow the empty

path $\emptyset$, where $m = 0$.

We call P an $s - t$ path if s is the tail of a_1 and t is the head of a_m. If $s = t$ we call P a *cycle*. If P is as in (3) then $P^{-1} := a_m^{-1} \cdots a_1^{-1}$.

3. Graph groups

3.1. Graph groups

Our method uses the framework of combinatorial group theory, viz. groups defined by generators and relations. For background literature on combinatorial group theory we refer to Magnus, Karrass, and Solitar [8] and Lyndon and Schupp [7]; however, our treatment below is self-contained.

We first give some standard terminology. Let $g_1, \ldots, g_k$ be 'generators'. Call the elements $g_1, g_1^{-1}, \ldots, g_k, g_k^{-1}$ *symbols*. Define $(g_i^{-1})^{-1} := g_i$. A *word* (of *size* t) is a sequence $a_1 \cdots a_t$ where each a_j is a symbol. The empty word (of size 0) is denoted by $\emptyset$. Define $(a_1 \cdots a_t)^{-1} := a_t^{-1} \cdots a_1^{-1}$.

Word y is a *segment* of word w if $w = xyz$ for words x, z; y is a *beginning segment* if $x = \emptyset$, and an *end segment* if $z = \emptyset$. Word $y = a_1 \cdots a_t$ is a *subword* of word w if $w = x_0 a_1 x_1 \cdots x_{t-1} a_t x_t$ for some words $x_0, \ldots, x_t$. It is a *proper* subword if $y \neq w$.

Let $g_1, \ldots, g_k$ be generators, and let E be a set of unordered pairs $\{i, j\}$ from $\{1, \ldots, k\}$ with $i \neq j$. Then the group $G = G_E$ is generated by the generators $g_1, \ldots, g_k$, with relations

(4) $\quad g_i g_j = g_j g_i$ for each pair $\{i, j\} \in E$.

Such a group is called a *free partially commutative group* or a *graph group*. (These groups are studied *inter alia* in [1], [4], [13], [18]. However, in this paper we do not use the results of these papers.)

To describe G, call symbols a and b *independent* if $a \in \{g_i, g_i^{-1}\}$ and $b \in \{g_j, g_j^{-1}\}$ for some $\{i, j\} \in E$ with $i \neq j$. So if a and b are independent then $ab = ba$ and $b \neq a^{\pm 1}$. (It follows from Proposition 3 below that also the converse implication holds.)

By definition, G consists of all words, identifying any two words w and w' if w' arises from w by iteratively:

(5) (i) replacing $xaa^{-1}y$ by xy or vice versa, where a is a symbol;
(ii) replacing $xaby$ by $xbay$ where a and b are independent symbols.

By *commuting* we will mean applying (ii) iteratively.

Note that if $E = \emptyset$ the group G_E is the *free group* generated by $g_1, \ldots, g_k$. If E consists of *all* pairs, then G_E is isomorphic to $\mathbb{Z}^k$. Let 1 denote the unit element of G. So $1 = \emptyset$.

A *perfect matching on* $\{1, \ldots, t\}$ is a partition of $\{1, \ldots, t\}$ into pairs. Pairs $\{i, j\}$ and $\{i', j'\}$ are said to *cross* if $i < i' < j < j'$ or $i' < i < j' < j$ (assuming without loss of generality $i < j, i' < j'$).

Proposition 1. *For any word $w = a_1 \cdots a_t$ one has: $w = 1$ if and only if there exists a*

perfect matching M on $\{1,\dots,t\}$ such that

(6) (i) *if $\{i,j\} \in M$ then $a_j = a_i^{-1}$;*
(ii) *if two pairs $\{i,j\},\{i',j'\}$ in M cross then a_i and $a_{i'}$ are independent.*

Proof. *Necessity.* If $w = \emptyset$ we can take $M = \emptyset$. Moreover, one easily shows that the existence of M is maintained under the operations (5).

Sufficiency. Let M satisfy (6). If $w \not\equiv \emptyset$, choose $\{i,j\} \in M$ with $i < j$ and $j - i$ as small as possible. Then a_i and $a_{i+1}\cdots a_{j-1}$ are independent, since each of the pairs containing one of $i+1,\dots,j-1$ should cross $\{i,j\}$.

Hence $w = a_1 \cdots a_{i-1}a_{i+1}\cdots a_{j-1}a_{j+1}\cdots a_t$. Since $M \setminus \{\{i,j\}\}$ directly gives a perfect matching for the right-hand word, we obtain inductively that $w = 1$. ∎

We call a word w *reduced* if it is not equal (as a word) to $xaya^{-1}z$ for some symbol a independent of y. We say that a symbol α *occurs in* an element x of G if α occurs in any reduced word representing x. We say that two words x and y are *independent* if any symbol in x and any symbol in y are independent. (In particular, $b \neq a^{\pm 1}$ for any symbols a in x and b in y.) Note that reducedness is invariant under commuting.

Proposition 1 directly implies:

Proposition 2. *If w is a reduced word and $w = 1$, then $w \equiv \emptyset$.*

Proof. If $w \not\equiv \emptyset$ and $w = 1$ one shows, as in the proof of Proposition 1, that w is not reduced. ∎

So testing if $w = 1$ is easy: just replace (iteratively) any segment aya^{-1} by y where a is a symbol and y is a word independent of a. The final word is empty if and only if $w = 1$. This gives a test for equivalence of words w and x: just test if $wx^{-1} = 1$. So the 'word problem' for free partially commutative groups is easy. (In fact it can be solved in linear time — see Wrathall [18].)

Proposition 2 also implies the stronger statement:

Proposition 3. *Let w and x be reduced words with $w = x$. Then word x can be obtained from w by a series of commutings.*

Proof. We may assume $w \not\equiv \emptyset \not\equiv x$. Since $wx^{-1} = 1$, wx^{-1} is not reduced. So we can write $w = w'aw''$ and $z = z'az''$ for some symbol a independent of w'' and z''. By commuting we may assume $w'' \equiv z'' \equiv \emptyset$. Then w' and x' are reduced equivalent words, and by induction w' and x' can be obtained from each other by a series of commutings. ∎

Proposition 3 implies:

(7) if $xyz = xy'z$ are reduced words then y' can be obtained from y by commuting

(since y and y' are reduced and $y = y'$.)

In particular, all equivalent reduced words have the same size. So we can define the *size* $|x|$ of an element x in G as the size of any reduced word $w = x$. Trivially, $|x^{-1}| = |x|$ and $|xy| \leq |x| + |y|$. Hence the function $\mathrm{dist}(x, y) := |x^{-1}y|$ is a distance function. Note that $\mathrm{dist}(zx, zy) = \mathrm{dist}(x, y)$ for all x, y, z.

We write

(8) $$x|y \iff |xy| = |x| + |y|.$$

So

(9) $x|y \iff$ if x' and y' are reduced words representing x and y, then $x'y'$ is a reduced word representing xy.

By extension we write:

(10) $$x_1|x_2|\cdots|x_n \iff |x_1x_2\cdots x_n| = |x_1| + |x_2|\cdots + |x_n|.$$

3.2. The partial order $\leq$

Let x and y be two reduced words. We write $x \leq y$ if there are reduced words $x' = x$ and $y' = y$ such that x' is a beginning segment of y'. So $x \leq y$ if and only if $x|x^{-1}y$.

Proposition 3 gives:

(11) if x and y are reduced words such that $x \leq y$ then y can be commuted to y' such that x is a beginning segment of y'.

This implies:

Proposition 4. *$\leq$ is a partial order on G.*

Proof. Clearly $x \leq x$ for each $x \in G$, so $\leq$ is reflexive. To see that $\leq$ is anti-symmetric, let $x \leq y$ and $y \leq x$. We may assume that x and y are reduced words. Then (11) implies that x and y can be commuted to each other. So $x = y$.

To see that $\leq$ is transitive, let $x \leq y$ and $y \leq z$, where x, y and z are reduced words. By (11) z can be commuted to z' such that y is beginning segment of z', and y can be commuted to y' such that x is beginning segment of y'. Hence z' can be commuted to z'' such that x is beginning segment of z''. Therefore $x \leq z$. ∎

Note that for all $x, y \in G$:

(12) $x \leq y$ if and only if $y^{-1}x \leq y^{-1}$.

Moreover, for all $x, y, z \in G$:

(13) if $x \leq y \leq z$ then $x^{-1}y \leq x^{-1}z, z^{-1}y \leq z^{-1}x$, and $x \leq zy^{-1}x$.

This implies:

Proposition 5. *For all $x, y, z \in G$, if $xy \leq z$ and $x|y$ then $x \leq zy^{-1}$.*

Proof. Since $x \leq xy \leq z$, by (13) we have $x \leq z(xy)^{-1}x = zy^{-1}$. ∎

In fact, the partial order $\leq$ yields a lattice if we add to G an element ∞ at infinity. First consider the following algorithm. For any $x \in G$ let *first*(x) denote the set of symbols α with $\alpha \leq x$.

For any two reduced words x and y the algorithm is as follows:

(14) Grow a reduced word z such that $zx' = x$ and $zy' = y$, where zx' and zy' are reduced words. Initially, $z := \emptyset$. If z has been found, choose a symbol $\alpha \in \mathit{first}(x') \cap \mathit{first}(y')$, reset $z := z\alpha$, remove the first occurrences of α from x' and y', and iterate. Stop if no such a exists.

Clearly the final z is reduced (as it is a beginning segment of a word arising by commuting x) and satisfies $z \leq x$ and $z \leq y$. Note that $\mathit{first}(x') \cap \mathit{first}(y') = \emptyset$ if and only if the word $y'^{-1}x'$ is reduced. Moreover:

Proposition 6. *If $w \leq x$ and $w \leq y$ then $w \leq z$.*

Proof. We may assume that w is a reduced word. Apply the algorithm (14) to w and z. We end up with reduced words $vz' = z$ and $vw' = w$ such that $\mathit{first}(w') \cap \mathit{first}(z') = \emptyset$. If $w' \equiv \emptyset$ then $w \leq z$, so assume $w' \not\equiv \emptyset$. Let x' and y' be as found in (14) applied to x and y. So $vz'x' = x$ and $vz'y' = y$ are reduced words. Since $vw' = w \leq x = vz'x'$ the first symbol a (say) of w' belongs to $\mathit{first}(z'x')$. Similarly, a belongs to $\mathit{first}(z'y')$. Since $a \notin \mathit{first}(z')$ it follows that a and z' are independent and that a belongs to $\mathit{first}(x') \cap \mathit{first}(y')$. This contradicts the construction of z. ∎

It follows that $\leq$ forms a lattice on $G \cup \{\infty\}$, with $x \wedge y = z$ where z is constructed as in (14). Note that (14) also gives an algorithm to test if $x \leq y$ for any two words. Moreover:

(15) for all $x, y \in G$: $x^{-1}(x \wedge y) \leq x^{-1}y$.

This follows from the fact that if z, x' and y' are as constructed in (14) then $(x')^{-1} = x^{-1}(x \wedge y)$ and $(x')^{-1}y' = x^{-1}y$, while $(x')^{-1}y'$ is a reduced word.

One has $x \vee y$ is finite (i.e., belongs to G) if and only if there is a $w \in G$ with $x \leq w$ and $y \leq w$. The following proposition describes how to find $x \vee y$. Let x and y be reduced. Let z, x' and y' be as constructed in (14).

Proposition 7. *If x' and y' are independent then $x \vee y$ is finite and is equal to $zx'y'$. Otherwise, $x \vee y = \infty$.*

Proof. If x' and y' are independent, then $zx'y' = zy'x'$ is a reduced word and $x = zx' \leq zx'y'$ and $y = zy' \leq zy'x'$.

Now let $zx' \leq w$ and $zy' \leq w$ for some reduced word w. Then w can be commuted to $zx'w'$ and to $zy'w''$, where $x'w'$ and $y'w''$ can be commuted to each other. Since $w''^{-1}y'^{-1}x'w' = 1$ there exists a perfect matching M satisfying (6). As $x'w'$ and $y'w''$ are reduced, each symbol in the $w''^{-1}y'^{-1}$ part is matched with a symbol in the $x'w'$ part. Since $\mathit{first}(x') \cap \mathit{first}(y') = \emptyset$, the symbols in the y'^{-1} part are not matched with the symbols in the x' part. So x' and y' are independent and hence $zx'y'$ is a reduced word and $zx'y' \leq w$. ∎

This directly implies that for any $x, y \in G$ with $x \vee y$ finite:

(16) $$x \vee y = x(x \wedge y)^{-1}y \text{ and } x \wedge y = x(x \vee y)^{-1}y.$$

Note that:

(17) $$\text{if } x \leq z \text{ and } y \leq z \text{ then } x \vee y = z(z^{-1}x \wedge z^{-1}y) \text{ and } x \wedge y = z(z^{-1}x \vee z^{-1}y).$$

The reason is that by (13) the function $w \mapsto z^{-1}w$ reverses the partial order on the set $\{w \in G \mid w \leq z\}$. Hence $z^{-1}(x \vee y) = z^{-1}x \wedge z^{-1}y$ and $z^{-1}(x \wedge y) = z^{-1}x \vee z^{-1}y$ whenever $x, y \leq z$.

We also note the following:

Proposition 8. *Let $x_1, \dots, x_t \in G$ be such that $x_i \vee x_j$ is finite for all i, j. Then $x_1 \vee \cdots \vee x_t$ is finite.*

Proof. Let $x_1, \dots, x_t$ be a counterexample with t as small as possible. So $x_1 \vee \cdots \vee x_t = \infty$ and $t \geq 3$. By the minimality of t each pair from $x_1 \vee x_4 \vee \cdots \vee x_t, x_2 \vee x_4 \vee \cdots \vee x_t, x_3 \vee x_4 \vee \cdots \vee x_t$ has finite join. If $t \geq 4$ this implies by the minimality of t that $x_1 \vee x_2 \vee x_3 \vee x_4 \vee \cdots \vee x_t$ is finite, a contradiction. So $t = 3$.

Assume we have chosen x_1, x_2, x_3 so that $|x_1| + |x_2| + |x_3|$ is as small as possible. Then x_1, x_2 and x_3 are reduced nonempty words. Write $x_1 \equiv y_1\alpha, x_2 \equiv y_2\beta, x_3 \equiv y_3\gamma$ where α, β, γ are symbols.

By the minimality condition, $z := y_1 \vee y_2 \vee y_3$ and $z \vee x_1$ are finite. If $z \vee x_1 = z$ then $x_1 \vee x_2 \vee x_3 = y_1 \vee x_2 \vee x_3$ is finite by the minimality condition. So $z \vee x_1 \neq z$. Since $y_1 \leq z$ we know $z = y_1 z'$ for some word z' with $y_1 | z'$. Hence, since $x_1 = y_1\alpha$ with $y_1|\alpha$, $z \vee x_1 = za$. Similarly $z \vee x_2 = zb$ and $z \vee x_3 = zc$. Moreover $a \neq b$, since otherwise $x_1 \vee x_2 \vee x_3 = za \vee zb \vee zc = za \vee zc = x_1 \vee y_2 \vee x_3$ is finite.

Since $za \vee zb = x_1 \vee x_2 \vee y_3$ is finite, a and b are independent. Similarly a and c are independent and b and c are independent. So $za, zb, zc \leq zabc = zbac = zcab$, and hence $x_1 \vee x_2 \vee x_3 = za \vee zb \vee zc$ is finite. ∎

The partial order $\leq$ is clearly not invariant under mappings $x \mapsto zx$ for $z \in G$. The following formula expresses how $\wedge$ behaves under such an operation.

Proposition 9. *For all $x, y, z \in G$ one has $z^{-1}x \wedge z^{-1}y = z^{-1}((x \wedge y) \vee (x \wedge z) \vee (y \wedge z))$.*

Proof. We may assume $x \wedge y \wedge z = 1$ (we can replace x by $(x \wedge y \wedge z)^{-1}x$, y by $(x \wedge y \wedge z)^{-1}y$,

and z by $(x \wedge y \wedge z)^{-1}z$). Let $u := x \wedge y, v := x \wedge z$ and $w := y \wedge z$. Since $u \wedge v = 1$ and $u \vee v$ is finite, u and v are independent. Similarly, u and w are independent and v and w are independent. So $(x \wedge y) \vee (x \wedge z) \vee (y \wedge z) = uvw$. Let $x' := (uv)^{-1}x, y' := (uw)^{-1}y$ and $z' := (vw)^{-1}z$. So uvx', uwy' and vwz' represent x, y and z as reduced words. Hence $(z')^{-1}w^{-1}ux' = (z')^{-1}uw^{-1}x'$ and $(z')^{-1}v^{-1}uy' = (z')^{-1}uv^{-1}y'$ represent $z^{-1}x$ and $z^{-1}y$ as reduced words. Now $w^{-1}x' \wedge v^{-1}y' = 1$ as $(w^{-1}x')^{-1}v^{-1}y' = (x')^{-1}v^{-1}wy'$ is a reduced word. Hence $z^{-1}x \wedge z^{-1}y = (z')^{-1}u = z^{-1}uvw$. ∎

It follows from Proposition 9 that $(x \wedge y) \vee (x \wedge z) \vee (y \wedge z)$ is the unique element w that is on the three shortest paths (with respect to the distance function dist) from x to y, x to z, and y to z. So $(x \wedge y) \vee (x \wedge z) \vee (y \wedge z)$ is the 'median' in the sense of Sholander [15,17, 16] (cf. [2]).

3.3. Join-irreducible elements and partial distributivity of G

It is helpful to see that each element of a free partially commutative group has an underlying partial order — extending the idea that the symbols in a word in the free group are totally ordered.

Let $\alpha_1 \cdots \alpha_t$ be a reduced word representing element x of G. Define a partial order $\preceq$ on $\{1, \ldots, t\}$ by:

(18) $i \preceq i' \Leftrightarrow$ there exist $i_0 = i < i_1 < \cdots < i_s = i'$ (with $s \geq 0$) such that $a_{i_{j-1}}$ and a_{i_j} are not independent, for each $j = 1, \ldots, s$,

for $i, i' \in \{1, \ldots, t\}$.

There is a one-to-one correspondence between linear extensions $i_1, \ldots, i_t$ of $1, \ldots, t$ (with respect to $\preceq$) and reduced words representing x. Here we define a *linear extension* with respect to $\preceq$ as a permutation $i_1, \ldots, i_t$ of $1, \ldots, t$ such that if $i_j \preceq i_{j'}$ then $j \leq j'$, for all $j, j' \in \{1, \ldots, t\}$.

For any linear extension $i_1, \ldots, i_t$ the word $w := \alpha_{i_1} \cdots \alpha_{i_t}$ is a reduced word representing x. This follows from the fact that any linear extension can be obtained from $1, \ldots, t$ by iteratively choosing two consecutive elements i_j, i_{j+1} with $i_j \not\preceq i_{j+1}$ and replacing them by i_{j+1}, i_j. So w arises by commuting from $\alpha_1 \cdots \alpha_t$.

Conversely, let $\alpha_{i_1} \cdots \alpha_{i_t}$ be a reduced word representing x, where $i_1, \ldots, i_t$ is a permutation of $1, \ldots, t$. We may assume that we have chosen indices such that if $\alpha_{i_j} = \alpha_{i_{j'}}$ and $j < j'$ then $i_j < i_{j'}$. Then $i_1, \ldots, i_t$ is a linear extension with respect to $\preceq$. This follows iteratively from the fact that if α_{i_j} and $\alpha_{i_{j+1}}$ are independent, then $i_j \not\preceq i_{j+1}$; thus if $i_1, \ldots i_j i_{j+1} \cdots i_t$ is a linear extension, then so is $i_1 \cdots i_{j+1} i_j \cdots i_t$.

Let L_x denote the set of lower ideals of $(\{1, \ldots, t\}, \preceq)$. (A subset I of $\{1, \ldots, t\}$ is a *lower ideal* if $i \in I$ and $j \preceq i$ implies $j \in I$.) Then the partially ordered sets $(L_x, \subseteq)$ and $(\{y \in G \mid y \leq x\}, \leq)$ are isomorphic. The isomorphism is given as follows. Let $y \leq x$. Then there is a linear extension $i_1, \ldots, i_t$ and an $s \leq t$ such that $\alpha_{i_1} \cdots \alpha_{i_s}$ is a reduced word representing y. Then $\{i_1, \ldots, i_s\}$ is a lower ideal of $\{1, \ldots, t\}$. (Indeed, if $i_j \preceq i_{j'}$ then $j \leq j'$; so if moreover $j' \leq s$ then $j \leq s$.) Conversely, for each lower ideal I of $\{1, \ldots, t\}$ there exists a linear extension $i_1, \ldots, i_t$ and an $s \leq t$ such that $I = \{i_1, \ldots, i_s\}$. Then

$\alpha_{i_1} \cdots \alpha_{i_s}$ is a reduced word representing an element $y \leq x$. It is not difficult to see that this gives a one-to-one correspondence, bringing $\leq$ to $\subseteq$.

In particular it follows that (cf. [2])

Proposition 10. *For each $x \in G$, the set $\{y \in G \mid y \leq x\}$, partially ordered by $\leq$, forms a distributive lattice.*

(That is, if $a, b, c \leq x$ then $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ and $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.)

Proof. This follows directly from the facts that the partially ordered sets $(\{y \in G \mid y \leq x\}, \leq)$ and $(L_x, \subseteq)$ are isomorphic and that the collection L_x is closed under taking unions and intersections. ∎

(The whole lattice on $G \cup \{\infty\}$ is generally not distributive: if a and b are distinct generators then $a \wedge (b \vee b^{-1}) = a \wedge \infty = a$ while $(a \wedge b) \vee (a \wedge b^{-1}) = 1 \vee 1 = 1$.)

As a corollary we have:

Proposition 11. *If $y \vee z$ is finite then $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$. If $x \vee y$ and $x \vee z$ are finite then $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$.*

Proof. The first line follows from the fact that taking $x' := x \wedge (y \vee z) \leq y \vee z$ we have $x', y, z \leq y \vee z$, implying $x' = (x' \wedge y) \vee (x' \wedge z) = (x \wedge y) \vee (x \wedge z)$. The second line follows from $(x \vee y) \wedge (x \vee z) = ((x \vee y) \wedge x) \vee ((x \vee y) \wedge z) = x \vee ((x \wedge z) \vee (y \wedge z)) = x \vee (y \wedge z)$ (using the first line). ∎

The correspondence also gives a correspondence for join-irreducible elements of G. An element x of G is called *join-irreducible* or a *left-interval* if $x \neq 1$ and if $y \vee z = x$ implies $y = x$ or $z = x$. Clearly, each element x of G is equal to the join of all join-irreducible elements $y \leq x$. Moreover, x is join-irreducible if and only if the partial order $\preceq$ defined above has a unique maximum element. In other words:

Proposition 12. *x is join-irreducible if and only if $x \neq 1$ and there exists a symbol α such that each reduced word representing x has last symbol equal to α.*

Proof. To see necessity, let x be join-irreducible. Let v and w be reduced words representing x, with last symbols α and β, respectively. If $\alpha \neq \beta$ then $x\alpha^{-1} \neq x\beta^{-1}$. Hence $x\alpha^{-1} \vee x\beta^{-1} = x$, contradicting the fact that x is join-irreducible.

To see sufficiency, let $x \neq 1$ and let there be a symbol α such that each reduced word representing x has last symbol equal to α. Moreover, let $x = y \vee z$. Then $x = x'y'z'$, where $x' := y \wedge z, y' := x'^{-1}y$ and $z' := x'^{-1}z$, $x'|y'|z'$ and y' and z' independent. So not both y' and z' can have α as last symbol, implying that $y' = 1$ or $z' = 1$. Therefore $z = x$ or $y = x$. ∎

Let J_x denote the collection of join-irreducible elements $y \leq x$. Then:

Proposition 13. *The partially ordered sets $(J_x, \leq)$ and $(\{1, \ldots, t\}, \preceq)$ are isomorphic.*

Proof. By the above, the join-irreducible elements correspond to lower-ideals of $\{1, \ldots, t\}$

that have a unique maximum element. So they are determined by their maximum element, and we have the required correspondence. ∎

It follows that:

Proposition 14. *For each $x \in G$, the number of join-irreducible elements $y \leq x$ is equal to $|x|$.*

Proof. Directly from Proposition 13. ∎

3.4. Cyclically reduced words and periodicity

Call an element a of G *cyclically reduced* if $a \wedge a^{-1} = 1$. So a is cyclically reduced if and only if $a|a$. Note that for each element a of G there exist unique b, c such that $a = bcb^{-1}$ with $b|c|b^{-1}$ and c cyclically reduced. In fact, $b = a \wedge a^{-1}$.

Proposition 15. *Let $x, a \in G$, where x is a left-interval with maximum symbol α and where α occurs in a. Assume $x \leq ax$ and $b \wedge x = 1$. Write $a = bcb^{-1}$ with $b|c|b^{-1}$ and c cyclically reduced. Then x and b are independent and $x \leq c^t$ for some t.*

Proof. Let $e := a^{-1} \wedge x$. Then $x \leq ax$ and $e|e^{-1}x$, and hence by Proposition 5 $e \leq ae$. Since $ae \leq a$, we have $e = e \wedge a = a^{-1} \wedge x \wedge a = b \wedge x = 1$. So $a \leq ax$. Hence $b \leq a \leq ax$ and $x \leq ax$, and therefore $b \vee x < \infty$, and so b and x are independent, and α occurs in c.

We next show that $x \leq c^t$ for some t by induction on $|x|$. We may assume that $x \not\leq c$. Moreover $x \wedge c \neq 1$, since $x \leq cx$ and $c \leq cx$, and hence if $x \wedge c = 1$ then x and c are independent, but both contain α.

Let $x' := (x \wedge c)^{-1}x$ $c' := (x \wedge c)^{-1}c(x \wedge c)$ and $a' := (x \wedge c)^{-1}a(x \wedge c) = bc'b^{-1}$. Then $x' \leq a'x'$, α occurs in a' and $b \wedge x' = 1$ (as b and x are independent). So by induction we know that $x' \leq (c')^s$ for some s. Hence $x \leq c^{s+1}$. ∎

Proposition 16. *Let a be cyclically reduced and let $x \in G$. Then $x \leq a^t$ for some t, if and only if there exist $a_t \leq a_{t-1} \leq \cdots \leq a_2 \leq a_1 \leq a$ such that $x = a_1 a_2 \cdots a_{t-1} a_t$ and $a_1|a_2|\cdots|a_{t-1}|a_t$ and such that a_i and $a_{i-1}^{-1}a$ are independent for each $i = 2, \ldots, t$.*

Proof. Sufficiency being easy, we show necessity. This is shown by induction on t, the case $t = 1$ being trivial. Let $a_1 := a \wedge x$ and $x' := a_1^{-1}x, b := a_1^{-1}a$. Since $a \leq a^t$ and $x \leq a^t$ we know that $a \vee x$ is finite, and hence b and x' are independent. So $x' \leq a^{t-1}$ since $x' \leq ba^{t-1}$ and b and x' are independent. So by induction there exist $a_t \leq a_{t-1} \leq \cdots \leq a_2 \leq a$ such that $x' = a_2 \cdots a_{t-1} a_t$ and $a_2|\cdots|a_{t-1}|a_t$ and such that a_i and $a_{i-1}^{-1}a$ are independent for each $i = 3, \ldots, t$. Since x' and b are independent we know in fact that $a_2 \leq a_1$ and that a_2 and $a_1^{-1}a$ are independent. Thus we have the required $a_1, \ldots, a_t$. ∎

Let $a \in G$. An element $d \in G$ is called a *component* of a if d is a minimal element with the properties that $1 \neq d \leq a$ and that d and $d^{-1}a$ are independent. So if $d_1, \ldots, d_n$ are the components of a then $a = d_1 \cdots d_n$ where the d_i are pairwise independent.

Proposition 17. *Let $a, x \in G$ be such that x is a left-interval with maximum symbol α,*

such that $x \le ax$ and such that $x^{-1}ax$ contains α. Let p be a natural number satisfying $p < \frac{|x|}{|a|} - |a|$. Let y be the component of $x^{-1}ax$ containing α. Then $x = ry^p$ where r is a left-interval with maximum symbol α, and $r|y^p$.

Proof. I. Write $a = bcb^{-1}$ with $b|c|b^{-1}$ and c cyclically reduced. First assume that $b = 1$. Then by Proposition 15 $x \le c^t$ for some t. By Proposition 16, there exist $c_t \le c_{t-1} \le \cdots \le c_2 \le c_1 \le c$ such that $x = c_1c_2\cdots c_{t-1}c_t$ and $c_1|c_2|\cdots|c_{t-1}|c_t$ and such that c_i and $c_{i-1}^{-1}c$ are independent for $i = 2,\ldots,t$. We may assume that $c_t \ne 1$. As $t \ge |x|/|c| > |c| + p$, there exists an $h \ge p+1$ such that $c_h = c_{h-1}$. Hence c_h and $c_h^{-1}c$ are independent. Let $d := c_h$ and $q := c_h^{-1}c$. Then $c_1 = \cdots = c_h = d$. Let $r := c_{h+1}\cdots c_t$. Then $x = d^h r$ and $r \le x$ (by Proposition 16). Hence $x = r(x^{-1}dx)^h$ (since $r^{-1}x = r^{-1}d^h r = (r^{-1}dr)^h = (x^{-1}dx)^h$.) Moreover, $r|(x^{-1}dx)^h$.

Now r is a left-interval with maximum symbol α, since r is an end-segment of x. Since x and q are independent, we have $x^{-1}ax = x^{-1}dxq$ with $x^{-1}dx$ and q independent, and therefore $x^{-1}dx = y$. In particular, $x = ry^{p+1}$ with $r|y^{p+1}$.

II. We now delete the assumption that $b = 1$. Let $x' := (b\wedge x)^{-1}x$, $b' := (b\wedge x)^{-1}b$ and $a' := (b\wedge x)^{-1}a(b\wedge x)$. By Proposition 15, b' and x' are independent. Moreover, $x' \le cx'$, since $x' \le a'x' = b'c(b')^{-1}x' = b'cx'(b')^{-1}$. Since moreover, $|x'| \ge |a'|^2 + p|a'| + |a'|$, we know by Section 3 that $x' = r'(y')^{p+1}$, and $r'|(y')^{p+1}$, where y' is the component of $(x')^{-1}cx'$ containing α, and where r is a left-interval with maximum symbol α.

Let y'' be such that $(x')^{-1}cx' = y'y''$. Since b' and x' are independent, also b' and y' are independent. So $x^{-1}ax = (x')^{-1}a'x' = (x')^{-1}b'c(b')^{-1}x' = b'(x')^{-1}cx'(b')^{-1} = b'(y'y'')(b')^{-1} = y'b'y''(b')^{-1})$ where y' and $b'y''(b')^{-1}$ are independent. So $y' = y$.

Now $b\wedge x|x'$ and $r'|y|y^p$ and hence $b\wedge x|r'|y|y^p$. Now $r := (b\wedge x)r'y$ is a left-interval with maximum symbol α. For let $\beta \ne \alpha$ be a maximum symbol of r. As $r'y$ is a left-interval with maximum symbol α, and as $r'|y$, β is a maximum symbol of $b\wedge x$ such that β and $r'y$ are independent. Then β and $r'y^{p+1}$ are independent, and hence β is also a maximum symbol of x. This contradicts the fact that x is a left-interval with maximum symbol α. ∎

3.5. Convex and closed sets

We call a subset H of G *left-convex* if H is nonempty and if $x, z \in H$ and $\mathrm{dist}(x,y) + \mathrm{dist}(y,z) = \mathrm{dist}(x,z)$ then $y \in H$. Since the distance function is invariant under functions $x \mapsto yx$, if H is left-convex also yH is left-convex for any $y \in G$.

Proposition 18. *A nonempty subset H of G is left-convex if and only if*

(19) (i) *if $x \le y \le z$ and $x, z \in H$ then $y \in H$;*
(ii) *if $x, y \in H$ then $x\wedge y \in H$ and, if $x\vee y$ is finite, $x\vee y \in H$.*

Proof. Necessity follows from the facts that if $x \le y \le z$ then $\mathrm{dist}(x,y) + \mathrm{dist}(y,z) = \mathrm{dist}(x,z)$, that $\mathrm{dist}(x,y) = \mathrm{dist}(x, x\wedge y) + \mathrm{dist}(x\wedge y, y)$ and that, if $x\vee y$ is finite then $\mathrm{dist}(x,y) = \mathrm{dist}(x, x\vee y) + \mathrm{dist}(x\vee y, y)$.

To see sufficiency, let $\mathrm{dist}(x,y) + \mathrm{dist}(y,z) = \mathrm{dist}(x,z)$ with $x, z \in H$. We must show $y \in H$. So $|x^{-1}y| + |y^{-1}z| = |x^{-1}z|$. This implies $x^{-1}y|y^{-1}z$. So $y^{-1}x \wedge y^{-1}z = 1$. Hence

by Proposition 9, $(x \wedge y) \vee (x \wedge z) \vee (y \wedge z) = y$. So $x \wedge z \leq x \wedge y \leq x$ and $x \wedge z \leq y \wedge z \leq z$. Therefore, $x \wedge y, x \wedge z$ and $y \wedge z$ belong to H and hence y belongs to H. ∎

In particular, each left-convex set has a unique minimum element. We call a subset H of G *right-convex* if H^{-1} is left-convex, and *convex* if H is both left- and right-convex. (As usual, $H^{-1} := \{x^{-1} \mid x \in H\}$.) We call a subset H of G *left-closed* if H is left-convex and $1 \in H$. It is *right-closed* if H^{-1} is left-closed, and *closed* if H is both left- and right-closed.

Proposition 19. *A nonempty subset H of G is left-closed if and only if*

(20) (i) *if $y \leq x$ and $x \in H$ then $y \in H$;*
(ii) *if $x, y \in H$ and $x \vee y$ is finite then $x \vee y \in H$.*

Proof. Directly from Proposition 18. ∎

Proposition 20. *If H is left-closed then for any $x \in G$: x belongs to H if and only if each left-interval of x belongs to H. If H is closed then for any $x \in G$: x belongs to H if and only if each interval of x belongs to H.*

Proof. Let H be left-closed. If $x \in H$ and y is a left-interval of x then $y \leq x$ and hence $y \in H$. The converse follows from the fact that $x = \bigvee\{y \mid y \text{ left-interval of } x\}$.

Let H be closed. If $x \in H$ and y is an interval of x then y is a segment of x and hence $y \in H$. Conversely, suppose that each interval of x belongs to H. Then each right-interval z of x belongs to H (since each left-interval w of z belongs to H as w is an interval of x). So by the first statement of the proposition applied to x^{-1} and H^{-1} we have $x \in H$. ∎

Clearly, the intersection of any number of left-convex sets is again left-convex. Moreover, left-convex sets satisfy the following 'Helly-type' property:

Proposition 21. *Let $H_1, \ldots, H_t$ be left-convex sets with $H_i \cap H_j \neq \emptyset$ for all $i, j = 1, \ldots, t$. Then $H_1 \cap \cdots \cap H_t \neq \emptyset$.*

Proof. Suppose not. Choose a counterexample with t minimal. If $t \geq 4$ then each two of $H_1 \cap H_4 \cap \cdots \cap H_t, H_2 \cap H_4 \cap \cdots \cap H_t, H_3 \cap H_4 \cap \cdots \cap H_t$ have a nonempty intersection (as it is an intersection of $t-1$ sets from $H_1, \ldots, H_t$). So these three sets have a nonempty intersection, a contradiction.

So $t = 3$. Choose $x \in H_1 \cap H_2, y \in H_1 \cap H_3, z \in H_2 \cap H_3$. Without loss of generality, $z = 1$ (as we can replace H_1, H_2, H_3 by $z^{-1}H_1, z^{-1}H_2, z^{-1}H_3$). Now $x \wedge y \in H_1 \cap H_2 \cap H_3$. ∎

Proposition 21 implies the following. As usual, define $HH' := \{xx' \mid x \in H, x' \in H'\}$.

Proposition 22. *Let H be left-convex and let H' and H'' be right-convex, with $H' \cap H'' \neq \emptyset$. Then $HH' \cap HH'' = H(H' \cap H'')$.*

Proof. Clearly $HH' \cap HH'' \supseteq H(H' \cap H'')$. To see the reverse inclusion, let $x \in HH' \cap HH''$.

So $x^{-1}H \cap H'^{-1} \neq \emptyset$ and $x^{-1}H \cap H''^{-1} \neq \emptyset$. Since also $H' \cap H'' \neq \emptyset$, by Proposition 21, $x^{-1}H \cap (H' \cap H'')^{-1} \neq \emptyset$. Hence $x \in H(H' \cap H'')$. ∎

For any left-convex H and $x \in G$, there is a unique element y in H 'closest' to x, that is, one minimizing $\mathrm{dist}(x, y)$. To see this we may assume H is left-closed. Then by (20) y is the largest element in H satisfying $y \leq x$.

We denote this element by $\mathrm{cl}_H(x)$. Then

Proposition 23. *Let H be left-convex and let H' be right-closed. Let $x \in G$ and $y := \mathrm{cl}_H(x)$. Then $x \in HH'$ if and only if $y^{-1}x \in H'$.*

Proof. Sufficiency being trivial, we prove necessity. We may assume that $y = 1$ (since replacing H by $y^{-1}H$ and x by $y^{-1}x$ does not modify the assertion). Hence H is left-closed. Let $x \in HH'$ and choose $w \in H, w' \in H'$ such that $x = ww'$ and such that $|w| + |w'|$ is as small as possible. We may assume that w and w' are reduced words. Then the word ww' is reduced again (since otherwise we could decrease $|w| + |w'|$). So $w \leq x$ and hence $w = 1$. Therefore, $x = w' \in H' \subseteq HH'$. ∎

Proposition 23 implies that if H is left-closed and H' is right-closed, and if we can test in polynomial time whether any given word x belongs to H and to H', then we can also test in polynomial time if any given word y belongs to HH'. We first find $z = \mathrm{cl}_H(x)$. This can be done as follows: if we have a reduced word $x'x'' = x$ with $x' \in H$, find a symbol $a \in \mathit{first}(x'')$ such that $x'a \in H$; reset $x' := x'a$, delete the first a from x'', and iterate. If no such a exists we set $z := x'$. Now by Proposition 23 $x \in HH'$ if and only if $y^{-1}x \in H'$.

Similarly, if H is left-convex and H' is right-convex and if we can test in polynomial time if any word belongs to H and to H' and moreover we know at least one word w in H and at least one word w' in H', then we can test if any given word x belongs to HH': we just test if $w^{-1}xw'^{-1}$ belongs to $(w^{-1}H)(H'w'^{-1})$. Note that $w^{-1}H$ is left-closed and that $H'w'^{-1}$ is right-closed.

Proposition 23 also implies:

Proposition 24. *Let H be left-convex and let H' be closed. Then HH' is left-convex.*

Proof. We may assume that H is left-closed. We show that HH' is left-closed. Let $x \in HH'$ and $y \leq x$. Let $u := \mathrm{cl}_H(x)$. So by Proposition 23, $u^{-1}x \in H'$. Moreover $(u \wedge y)^{-1}y \leq u^{-1}x$ (since $u \leq u \vee y \leq x$ and $u \vee y = u(u \wedge y)^{-1}y$). This implies $(u \wedge y)^{-1}y \in H'$ and hence, as $u \wedge y \in H$, $y \in HH'$.

Next let $x, y \in HH'$ with $x \vee y$ finite. Let $u := \mathrm{cl}_H(x)$ and $v := \mathrm{cl}_H(y)$. So $u^{-1}x$ and $v^{-1}y$ belong to H'. Now $(u \vee v)^{-1}(x \vee v) = (u \vee v)^{-1}(x \vee (u \vee v)) = (x \wedge (u \vee v))^{-1}x = u^{-1}x \in H'$ (since $x \wedge (u \vee v) = u$ as $u = \mathrm{cl}_H(x)$). Hence $x \vee v \in (u \vee v)H'$. Similarly $y \vee u \in (u \vee v)H'$. Hence $x \vee y = (x \vee v) \vee (y \vee u) \in (u \vee v)H' \subseteq HH'$. ∎

For any $x \in G$ define

(21) $$H_x^{\uparrow} := \{y \in G \mid y \geq x\} \text{ and } H_x^{\downarrow} := \{y \in G \mid y \leq x\}.$$

It is not difficult to see that $H_x^{\uparrow}$ and $H_x^{\downarrow}$ are left-convex.

Proposition 25. *Let H be closed and let $x, y, z \in G$. Then $x^{-1}yz$ belongs to H if and only if:* (i) $\exists u \leq x \; \exists w \leq z : u^{-1}yw \in H$; (ii) $\exists u \leq x \; \exists w \geq z : u^{-1}yw \in H$; (iii) $\exists u \geq x \; \exists w \leq z : u^{-1}yw \in H$; (iv) $\exists u \geq x \; \exists w \geq z : u^{-1}yw \in H$.

Proof. Necessity being trivial we show sufficiency. Assertion (i) means $y \in H_x^{\downarrow} H H_z^{\downarrow -1}$, and assertion (ii) means $y \in H_x^{\downarrow} H H_z^{\uparrow -1}$. Hence by Proposition 22, $y \in H_x^{\downarrow} H (H_z^{\downarrow -1} \cap H_z^{\uparrow -1}) = H_x^{\downarrow} H z^{-1}$. Similarly, $y \in H_x^{\uparrow} H z^{-1}$. Again by Proposition 22, $y \in (H_x^{\downarrow} \cap H_x^{\uparrow}) H z^{-1} = xHz^{-1}$. Therefore $x^{-1}yz \in H$. ∎

Proposition 26. *Let H be closed and let x, a be such that $x^{-1}ax \in H$. Then there exists a y such that $y^{-1}ay \in H$ and such that $y \leq a^t$ for some t.*

Proof. By induction on $|x|$. If $x \wedge ax \neq 1$, let α be a symbol satisfying $\alpha \leq x \wedge ax$. Let $x' := \alpha^{-1}x$ and $a' := \alpha^{-1}a\alpha$. Then $(x')^{-1}a'x' \in H$ and hence by induction there exists a y' such that $(y')^{-1}a'y' \in H$ and such that $y' \leq (a')^s$ for some s. Then $y := \alpha y'$ satisfies $y^{-1}ay = (y')^{-1}a'y' \in H$ and $y \leq \alpha(a')^s \leq a^{s+1}$.

Similarly, if $x^{-1} \wedge (a^{-1}x^{-1}) \neq 1$. Hence we may assume that $x^{-1}|a|x$. But then a is a segment of $x^{-1}ax$, and hence $a \in H$. This implies that we can take $y := 1$. ∎

This implies:

Proposition 27. *Let H be closed and let x, a be such that $x^{-1}a^sx \in H$ for some s. Then there exists a y such that $y^{-1}a^sy \in H$ and such that $y \leq a^{|a|}$.*

Proof. First assume that a is cyclically reduced. By Proposition 26 we may assume that $x \leq a^t$ for some t. We choose x and t such that t is minimal. We show that $t \leq |a|$. Assume $t > |a|$. By Proposition 16 there exist $1 \leq a_t \leq a_{t-1} \leq \cdots \leq a_2 \leq a_1 \leq a$ such that $x = a_1a_2 \cdots a_{t-1}a_t$ and $a_1|a_2| \cdots |a_{t-1}|a_t$ and such that a_i and $a_{i-1}^{-1}a$ are independent for each $i = 2, \ldots, t$. By the minimality of t, $a_t \neq 1$. As $t > |a|$ there exist an $i \in \{2, \ldots, t\}$ such that $a_{i-1} = a_i$. Then a_i and $a_i^{-1}a$ are independent. So $a_iaa_i^{-1} = a$. Hence for $x' := a_i^{-1}x$ we have $(x')^{-1}a^sx' = x^{-1}a^sx \in H$ and $x' \leq a^{t-1}$, since $x' = a_1a_2 \cdots a_{i-1}a_{i+1} \cdots a_t$. This contradicts the minimality of t.

If a is not cyclically reduced, let $a = bcb^{-1}$ with $b|c|b^{-1}$ and c cyclically reduced. Then for $x' := b^{-1}x$ we know that $(x')^{-1}c^sx'$ belongs to H, and hence there exists a y' such that $(y')^{-1}c^sy' \in H$ and such that $|y'| \leq c^{|c|}$. Then for $y := by'$ we have $y^{-1}a^sy \in H$ and $y \leq a^{|c|} \leq a^{|a|}$. ∎

4. The cohomology feasibility problem

4.1. The cohomology feasibility problem

Let $D = (V, A)$ be a directed graph and let G be a group. Two functions $\phi, \psi : A \to G$ are called *cohomologous* if there exists a function $p : V \to G$ such that $\psi(a) = p(u)^{-1}\phi(a)p(w)$ for each arc $a = (u, w)$. One directly checks that this gives an equivalence relation.

Consider the following *cohomology feasibility problem*:

(22) given: a directed graph $D = (V, A)$, a group G, a function $\phi : A \to G$, and for each $a \in A$, a subset $H(a)$ of G;
find: a function $\psi : A \to G$ such that ψ is cohomologous to ϕ and such that $\psi(a) \in H(a)$ for each $a \in A$.

We give a polynomial-time algorithm for this problem in case G is an free partially commutative group and each $H(a)$ is a closed set.

In the algorithm it is not required that the $H(a)$ are given explicitly. It suffices to be given an algorithm that tests for any a and any word x whether or not x belongs to $H(a)$. (So $H(a)$ might be infinite.) The running time of the algorithm for the cohomology feasibility problem is bounded by a polynomial in $n := |V|$, $\sigma := \max\{|\phi(a)| \mid a \in A\}$, and τ, where τ is the maximum time needed to test membership of x in $H(a)$ for any given arc a and any given word x of length bounded by a polynomial in n and σ. (The number k of generators can be bounded by $n\sigma$, since we may assume that all generators occur among the $\phi(a)$.)

Note that, by the definition of cohomologous, equivalent to finding a ψ as in (22), is finding a function $f : V \to G$ satisfying:

(23) $f(u)^{-1}\phi(a)f(w) \in H(a)$ for each arc $a = (u, w)$.

We call such a function f *feasible*.

Note that if f is feasible and P is an $s-t$ path, then $f(s)^{-1}\phi(P)f(t) \in H(P)$. Here for any path $P = a_1 \cdots a_m$ we use the following definitions:

(24)
$$\phi(P) := \phi(a_1) \cdots \phi(a_m),$$
$$H(P) := H(a_1) \cdots H(a_m),$$

where $\phi(a^{-1}) := \phi(a)^{-1}$ and $H(a^{-1}) = H(a)^{-1}$.

This gives an obvious necessary (but not sufficient) condition for problem (22) having a solution:

(25) for each cycle P there exists an $x \in G$ such that $x^{-1}\phi(P)x$ belongs to $H(P)$.

4.2. Pre-feasible functions

Let $D = (V, A)$ be a directed graph, let G be a group, let $\phi : A \to G$ and for each $a \in A$, let $H(a)$ be a closed subset of G.

We call a function $f : V \to G$ *pre-feasible* if for each arc $a = (u, w)$ of D there exist $x \geq f(u)$ and $z \leq f(w)$ such that $x^{-1}\phi(a)z \in H(a)$. Clearly, each feasible function is pre-feasible. There is a trivial pre-feasible function f, defined by $f(v) := 1$ for each $v \in V$.

The collection of pre-feasible functions is closed under certain operations on the set G_M^V of all functions $f : V \to G_M$. This set can be partially ordered by: $f \leq g$ if and only if

$f(v) \leq g(v)$ for each $v \in V$. Then G_M^V forms a lattice if we add an element ∞ at infinity. Let $\wedge$ and $\vee$ denote meet and join.

Proposition 28. *Let f_1 and f_2 be pre-feasible functions. Then $f_1 \wedge f_2$ and, if $f_1 \vee f_2 < \infty$, $f_1 \vee f_2$ are pre-feasible again.*

Proof. To see that $f_1 \wedge f_2$ is pre-feasible, choose an arc $a = (u, w)$. Since f_1 is pre-feasible, $\phi(a) \in H^{\uparrow}_{f_1(u)} H(a) (H^{\downarrow}_{f_1(w)})^{-1} \subseteq H^{\uparrow}_{f_1(u) \wedge f_2(u)} H(a) (H^{\downarrow}_{f_1(w)})^{-1}$. Similarly, $\phi(a) \in H^{\uparrow}_{f_1(u) \wedge f_2(u)} H(a) (H^{\downarrow}_{f_2(w)})^{-1}$. So by Proposition 22,

$$\phi(a) \in H^{\uparrow}_{f_1(u)\wedge f_2(u)} H(a) (H^{\downarrow}_{f_1(w)} \cap H^{\downarrow}_{f_2(w)})^{-1} = H^{\uparrow}_{f_1(u)\wedge f_2(u)} H(a) (H^{\downarrow}_{f_1(w)\wedge f_2(w)})^{-1}. \tag{26}$$

This means that there exist $x \geq f_1(u) \wedge f_2(u)$ and $z \leq f_1(w) \wedge f_2(w)$ such that $x^{-1}\phi(a)z \in H(a)$.

The fact that $f_1 \vee f_2$ is pre-feasible if it is not ∞, is shown similarly. ∎

It follows that for each function $f : V \to G$ there is a unique smallest pre-feasible function $\bar{f} \geq f$, provided that there exists at least one pre-feasible function $g \geq f$. If no such g exists we set $\bar{f} := \infty$. Note that $\overline{f \vee g} = \bar{f} \vee \bar{g}$ for any two functions f, g with $f \vee g$ finite.

4.3. A subroutine finding $\bar{f}$

Let input $D = (V, A), \phi, H$ for the cohomology feasibility problem be given. We describe a polynomial-time subroutine that outputs $\bar{f}$ for any given function f, under the assumption that (25) holds.

For any arc $a = (u, w)$ and any $x \in G$ let $\beta_a(x)$ be the smallest element z in G such that there exists an $x' \geq x$ with $(x')^{-1}\phi(a)z \in H(a)$. This is unique, as z is the minimum element in the left-convex set $\phi(a)^{-1} H^{\uparrow}_x H(a)$. Note that for any $f : V \to G$ one has:

$$f \text{ is pre-feasible if and only if } \beta_a(f(u)) \leq f(w) \text{ for each arc } a = (u, w). \tag{27}$$

For any given x we can determine $\beta_a(x)$ in polynomial time if we can test in polynomial time if any given word belongs to $H(a)$ (as $\beta_a(x)$ is the minimal element of $\phi(a)^{-1} H^{\uparrow}_x H(a)$).

Subroutine to find $\bar{f}$: If f is pre-feasible, output $\bar{f} := f$. Otherwise, choose an arc $a = (u, w)$ such that $\beta_a(f(u)) \not\leq f(w)$. If $f(w) \vee \beta_a(f(u)) = \infty$, output $\bar{f} := \infty$. Otherwise reset $f(w) := f(w) \vee \beta_a(f(u))$, and start anew.

Proposition 29. *The output in the subroutine is correct.*

Proof. Clearly, if $f(w) \vee \beta_a(f(u)) = \infty$ then $\bar{f} = \infty$. If $f(w) \vee \beta_a(f(u)) < \infty$, let f' denote the reset function. Then $f \leq f'$. Moreover, if $\bar{f}$ is finite, then $f \leq f' \leq \bar{f}$, since $f'(w) = f(w) \vee \beta_a(f(u)) \leq \bar{f}(w) \vee \beta_a(\bar{f}(u)) = \bar{f}(w)$, since $\bar{f}$ is pre-feasible. ∎

4.4. Running time of the subroutine

We show that after at most $2^{15}n^9k^9\sigma^8 + 2^2n^2k^2\rho$ iterations the subroutine gives an output, where:

$$
\begin{aligned}
(28)\qquad & n := |V|,\\
& \sigma := \max\{|\phi(a)| \mid a \in A\},\\
& \rho := \max\{|f(v)| \mid v \in V\}.
\end{aligned}
$$

To this end we first make some observations and introduce some further terminology.

Proposition 30. *$\beta_a(x \vee y) = \beta_a(x) \vee \beta_a(y)$ for all $x, y \in G$ with $x \vee y$ finite.*

Proof. Clearly, for all x, y, if $x \leq y$ then $\beta_a(x) \leq \beta_a(y)$. Equivalently, $\beta_a(x \vee y) \geq \beta_a(x) \vee \beta_a(y)$ for all x, y with $x \vee y$ finite. To see the reverse inequality, let $u := \beta_a(x)$ and $v := \beta_a(y)$. Since $x'^{-1}\phi(a)u \in H(a)$ for some $x' \geq x$, $H_x^{\uparrow} \cap \phi(a)H_{u\vee v}^{\downarrow}H(a)^{-1} \neq \emptyset$ (as x' belongs to it). Similarly, $H_y^{\uparrow} \cap \phi(a)H_{u\vee v}^{\downarrow}H(a)^{-1} \neq \emptyset$. Since also $H_x^{\uparrow} \cap H_y^{\uparrow} = H_{x\vee y}^{\uparrow} \neq \emptyset$, by Proposition 21 $H_{x\vee y}^{\uparrow} \cap \phi(a)H_{u\vee v}^{\downarrow}H(a)^{-1} \neq \emptyset$. Hence $\beta_a(x \vee y) \leq u \vee v$. ∎

Define for each path P in D and each $x \in G$, $\beta_P(x)$ inductively by: $\beta_\emptyset(x) := x$ and $\beta_{Pa}(x) := \beta_a(\beta_P(x))$. Inductively it follows from Proposition 30 that $\beta_P(x \vee y) = \beta_P(x) \vee \beta_P(y)$ for all $x, y \in G$ with $x \vee y$ finite. Moreover:

Proposition 31. *For each path P in D, each $x \in G$ and each $y \in H(P)$ we have $\beta_P(x) \leq \phi(P)^{-1}xy$.*

Proof. If $P = \emptyset$, the assertion is trivial. If $P = a$, then for $z := \phi(a)^{-1}xy$ one has $x^{-1}\phi(a)z = y \in H(a)$, and hence $\beta_a(x) \leq z = \phi(a)^{-1}xy$.

Consider next a path Pa and let $y = y'y'' \in H(Pa)$, with $y' \in H(P)$ and $y'' \in H(a)$. Then by induction,

$$
(29)\qquad \beta_{Pa}(x) = \beta_a(\beta_P(x)) \leq \beta_a(\phi(P)^{-1}xy') \leq \phi(a)^{-1}(\phi(P)^{-1}xy')y'' = \phi(Pa)^{-1}xy.
$$

∎

We introduce the following further structure. At each iteration t of the subroutine we maintain a collection Π_t of paths. Let f_t denote the function f as it is after t iterations. We first set $\Pi_0 := \{\emptyset\}$. If at iteration t we choose arc $a = (u, w)$ and put $f_t(w) := f_{t-1}(w) \vee \beta_a(f_{t-1}(u))$, then for each left interval $x \leq \beta_a(f_{t-1}(u))$ satisfying $x \not\leq f_{t-1}(w)$ we choose a left-interval $y \leq f_{t-1}(u)$ such that $x \leq \beta_a(y)$, and we set $P_{w,x} := P_{u,y}a$. (Such a y can be chosen by Proposition 30.) We add each such path to Π_{t-1}, thus obtaining Π_t.

Note that the collection Π_t has the following property:

(30) for each vertex v and each left-interval $x \leq f_t(v)$ there is a vertex r and an $r - v$ path $P_{v,x} \in \Pi_t$ such that $x \leq \beta_{P_{v,x}}(f(r))$.

Proposition 32. *The subroutine takes at most* $t := 2^{15}n^9k^9\sigma^8 + 2^2n^2k^2\rho$ *iterations.*

Proof. Suppose we have performed t iterations. We first show:

(31) Π_t contains a directed path P with $T := 2^{11}n^7k^7\sigma^6$ arcs.

First note that $|\Pi_t| \geq 2^{15}n^9k^9\sigma^8 + 2^2n^2k^2\rho$, since at each iteration at least one path is added. For each path $P_{v,x}$ in Π_t, with starting vertex r say, there exists a left-interval $y \leq f_0(r)$ such that $x \leq \beta_{P_{v,x}}(y)$. Since there are n vertices and $2k$ symbols, there exist vertices r, v and symbols α, β such that there are at least $t/(2nk)^2 = 2^{13}n^7k^7\sigma^8 + \rho$ join-irreducible elements x with the following properties:

(32) (i) $P_{v,x}$ belongs to Π_t and runs from r to v;
(ii) the maximum symbol of x is equal to α;
(iii) $x \leq \beta_{P_{v,x}}(y)$ for some left-interval $y \leq f_0(r)$ with maximum symbol β.

Let X denote the collection of such x. Since each $x \in X$ has maximum symbol α and satisfies $x \leq f_t(v)$, the elements in X form a chain (i.e., are totally ordered by $\leq$). Let w be the maximum element in X. Then

(33) $|w| \geq |X| \geq 2^{13}n^7k^7\sigma^8 + \rho.$

Let m be the number of arcs in $P_{v,w}$. Let z be the largest left-interval with maximum symbol β and satisfying $z \leq f_0(r)$. Then by Proposition 31, $w \leq \beta_{P_{v,w}}(z) \leq \phi(P_{v,w})^{-1}z$; so $|w| \leq |\phi(P_{v,w})| + |z| \leq m\sigma + \rho$. Hence with (33), $m \geq 2^{13}n^7k^7\sigma^7$. Since each beginning segment of a path in Π_t again belongs to Π_t we have (31).

Let P traverse vertices $v_0, v_1, \ldots, v_T$ in this order. By construction of Π_t we can find left-intervals $y_0, y_1, \ldots, y_T$ such that $y_0 \leq f_0(v_0)$ and $y_i \leq \beta_a(y_{i-1})$ where $a = (v_{i-1}, v_i)$ (for $i = 1, \ldots, T$). So P_{v_i,y_i} is the subpath of P consisting of the first i arcs of P.

For each vertex v of D and each symbol α let $I_{v,\alpha}$ denote the set of indices $i \in \{0, \ldots, T\}$ such that $v_i = v$ and such that y_i has maximum symbol α. Then there exists a vertex w of D and a symbol β such that $|I_{w,\beta}| \geq T/2nk$. Let L be the largest index in $I_{w,\beta}$. Since for all $i, i' \in I_{w,\beta}$ and $i < i'$ we have $y_i < y_{i'}$ (since y_i has maximum symbol β and satisfies $y_i \leq f_t(w)$ for each $i \in I_{w,\beta}$ and since $y_{i'} \not\leq y_i$), we know

(34) $|y_L| \geq |I_{w,\beta}| \geq T/2nk = 2^{10}n^6k^6\sigma^5.$

Let $M := 2^4n^3k^3\sigma^2$ and $N := 2^3n^2k^2\sigma^2$. Since $N = M/2nk$, there exists a vertex u and a symbol α such that $I_{u,\alpha}$ contains at least $N+1$ indices i satisfying $L - M \leq i \leq L$. Choose $N+1$ such indices $i_0 < i_1 < \cdots < i_N$. Define

(35) $x_0 := y_{i_0}, x_1 := y_{i_1}, \ldots, x_N := y_{i_N}.$

For $j = 1, \ldots, N$ let C_j be the $u-u$ path $v_{i_0}, v_{i_0+1}, \ldots, v_{i_j-1}, v_{i_j}$. We show that C_N violates (25). Note that

(36) $$|\phi(C_j)| \le (i_j - i_0)\sigma \le M\sigma = 2^5 n^3 k^3 \sigma^3$$

for each $j = 1, \ldots, N$.

Since $x_j \le f_t(u)$ and since α is the maximum symbol of x_j for each $j = 0, \ldots, N$, we know that $x_0 < x_1 < \cdots < x_N$. Moreover,

(37) $$x_0 < x_j \le \beta_{C_j}(x_0) \le \phi(C_j)^{-1} x_0$$

for each $j = 1, \ldots, N$ (by Proposition 31).

By Proposition 31, $y_L \le \beta_Q(x_0) \le \phi(Q)^{-1} x_0$, where Q denotes the path $v_{i_0}, v_{i_0+1}, \ldots, v_{L-1}, v_L$. Hence, taking $p := (M\sigma)^2$,

(38) $$|x_0| \ge |y_L| - |\phi(Q)| \ge 4(M\sigma)^3 - M\sigma \ge 3(M\sigma)^3 > |\phi(C_j)|^2 + p|\phi(C_j)|.$$

Write $\phi(C_j)^{-1} = b_j c_j b_j^{-1}$ with $b_j | c_j | b_j^{-1}$ and c_j cyclically reduced. Let y_j be the component of $x_0^{-1}\phi(C_j)^{-1}x_0$ containing α. Then by Proposition 17, y_j is cyclically reduced and

(39) $$x_0 = r_j y_j^p \text{ and } r_j | y_j^p,$$

such that r_j and y_j are left-intervals with maximum symbol α.

Let y_j have m_j symbols α and let x_0 have m symbols α. Write $x_0 = z_m z_{m-1} \cdots z_1$, where each z_i is a left-interval with maximum symbol α and where $z_m | z_{m-1} | \cdots | z_2 | z_1$. (Such a decomposition is unique.) By (39) we know that, for each $j = 1, \ldots, N$, $m \ge pm_j$ and that $z_i = z_{i'}$ if $i \equiv i' \pmod{m_j}$ and $i, i' \le pm_j$. Hence, for $m := \gcd\{m_1, \ldots, m_N\}$, $z_i = z_{i'}$ if $i \equiv i' \pmod{m}$ and $i, i' \le pm$.

Let $a := z_n z_{n-1} \cdots z_1$ and $n_j := m_j/m$ for $m = 1, \ldots, N$. Then $y_j = a^{n_j}$ for each $j = 1, \ldots, N$.

Write $x_0^{-1}\phi(C_j)^{-1}x_0 = y_j y_j'$ for some y_j' such that y_j and y_j' are independent. Since $x_0^{-1}x_j \le x_0^{-1}\phi(C_j)^{-1}x_0$ and since $x_0^{-1}x_j$ is a left-interval with maximum symbol α, we know that $x_0^{-1}x_j \le y_j$. As $y_j^{n_{j'}} = y_{j'}^{n_j}$ for all j, j', it follows that $x_0^{-1}x_j$ and $y_{j'}'$ are independent, for each j'.

Moreover,

(40) $$n_1 < n_2 < \cdots < n_N.$$

For suppose that $n_{j+1} \le n_j$ for some $j = 1, \ldots, N-1$. Let C be the closed path satisfying $C_{j+1} = C_j C$. Then $x_{j+1} \le \beta_C(x_j) \le \phi(C)^{-1}x_j$ and hence

(41) $$\begin{aligned} x_0^{-1}x_{j+1} &\le x_0^{-1}\beta_C(x_j) \le x_0^{-1}\phi(C)^{-1}x_j = x_0^{-1}\phi(C_{j+1})^{-1}\phi(C_j)x_j \\ &= (x_0^{-1}\phi(C_{j+1})^{-1}x_0)(x_0^{-1}\phi(C_j)x_0)(x_0^{-1}x_j) \\ &= a^{n_{j+1}}a^{-n_j}(x_0^{-1}x_j)((y_{j+1}')^{-1}y_j'), \end{aligned}$$

where $a^{n_{j+1}}a^{-n_j}(x_0^{-1}x_j)|((y_{j+1}')^{-1}y_j')$. This implies $x_{j+1} \le (x_0 a^{n_{j+1}-n_j})(x_0^{-1}x_j)$, and hence $|x_{j+1}| \le |x_0 a^{n_{j+1}-n_j}| + |x_0^{-1}x_j| \le |x_0| + |x_0^{-1}x_j| = |x_j|$. (The inequality $|x_0 a^{n_{j+1}-n_j}| \le |x_0|$

follows from the fact that $x_0 = fa^{n_j - n_{j+1}}$ for some f satisfying $f|a^{n_j-n_{j+1}}$, since $0 \leq m_j - m_{j+1} \leq m_j \leq M\sigma$.) This contradicts the fact that $x_{j+1} > x_j$, thus showing (40).

Now $|a| \leq M\sigma/N = 2nk\sigma$, since $|a^{n_N}| \leq M\sigma$ and $n_N \geq N$ (by (40)). By (25), there exists an $x \in G$ such that $x^{-1}\phi(C_N)x \in H(C_N)$. Hence there exists a $y \in G$ such that $y^{-1}a^{n_N}y \in H(C_N)^{-1}$. By Proposition 27 we may assume that $y \leq a^{|a|}$. Hence $a^{n_N-|a|} \in H(C_N)^{-1}$. Now by Proposition 31, $x_N \leq \beta_{C_N}(x_0) \leq \phi(C_N)^{-1}x_0a^{n_N-|a|}$, and hence $x_0^{-1}x_N \leq x_0^{-1}\beta_{C_N}(x_0) \leq x_0^{-1}\phi(C_N)^{-1}x_0a^{|a|-n_N} = a^{|a|}y'_N$, with $a^{|a|}|y'_N$. So $x_0^{-1}x_N \leq a^{|a|}$. Therefore $|x_0^{-1}x_N| \leq |a|^2 \leq (2nk\sigma)^2$. Since $x_0 < x_1 < \cdots < x_N$ we know $|x_0^{-1}x_N| \geq N$. Hence $2^3n^2k^2\sigma^2 = N \leq (2nk\sigma)^2$, a contradiction. ∎

Combining the propositions, we obtain that the running time of the subroutine is bounded by a polynomial in the input size and in the time needed to check membership of $H(a)$. Then:

Theorem 1. *The running time of the subroutine is bounded by a polynomial in n, k, σ and τ, where τ is the maximum time necessary to test if any word of size at most $\rho + 2^{24}n^{12}k^{12}\sigma^{11}$ belongs to any $H(a)$.*

Proof. Since initially $|f(v)| \leq \rho$ for each vertex v, we have after t iterations $|f_t(v)| \leq \rho + \sigma t$ for each vertex v. Since we do at most $2^{24}n^{12}k^{12}\sigma^{10}$ iterations, the result follows. ∎

4.5. A polynomial-time algorithm for the cohomology feasibility problem for free partially commutative groups

We now describe the algorithm for the cohomology feasibility problem for free partially commutative groups. Let $D = (V, A)$ be a directed graph, let G be a free partially commutative group, let $\phi : A \to G$ and let $H(a)$ be a closed subset of G, for each $a \in A$. We assume that with each arc $a = (u, w)$ also $a^{-1} = (w, u)$ is an arc, with $\phi(a^{-1}) = \phi(a)^{-1}$ and $H(a^{-1}) = H(a)^{-1}$.

Let $\mathcal{U}$ be the collection of all functions $f : V \to G$ such that for each arc $a = (u, w)$ there exist $x \geq f(u)$ and $z \geq f(w)$ satisfying $x^{-1}\phi(a)z \in H(a)$. For any given function f one can check in polynomial time whether f belongs to $\mathcal{U}$. Trivially, if $f \in \mathcal{U}$ and $g \leq f$ then $g \in \mathcal{U}$. Moreover:

Proposition 33. *Let $f_1, \ldots, f_t$ be functions such that $f_i \vee f_j \in \mathcal{U}$ for all i, j. Then $f := f_1 \vee \cdots \vee f_t \in \mathcal{U}$.*

Proof. Choose an arc $a = (u, w)$. We must show that for each arc $a = (u, w)$, $\phi(a)$ belongs to $H^{\uparrow}_{f(u)}H(a)(H^{\uparrow}_{f(w)})^{-1}$. Since $f_i \vee f_j \in \mathcal{U}$ for all i, j, we know

$$\phi(a) \in H^{\uparrow}_{f_i(u)}H(a)(H^{\uparrow}_{f_j(w)})^{-1} \tag{42}$$

for all i, j. Hence by Proposition 22

$$\phi(a) \in \bigcap_i \bigcap_j (H^{\uparrow}_{f_i(u)}H(a)(H^{\uparrow}_{f_j(w)})^{-1}) \tag{43}$$

$$= (\bigcap_i H^{\uparrow}_{f_i(u)})H(a)(\bigcap_j H^{\uparrow}_{f_j(w)})^{-1} = H^{\uparrow}_{f(u)}H(a)(H^{\uparrow}_{f(w)})^{-1}$$

Here i and j range over $1, \ldots, t$. ∎

Let X be the set of pairs (u, x) where $u \in V$ and where x is a left-interval such that there exists an arc $a = (u, w)$ with $x \leq \phi(a)$. So X has size polynomially bounded by n and σ. For any $(u, x) \in X$, let $f_{u,x}$ be the function defined by

(44)
$$\begin{aligned} f_{u,x}(u) &:= x, \\ f_{u,x}(v) &:= 1 \text{ for all } v \neq u. \end{aligned}$$

Let E be the set of pairs $\{(u, x), (w, z)\}$ from X such that there exists an arc $a = (u, w)$ such that

(45) $\quad$ for all $x', z' \in G$, if $(x')^{-1}\phi(a)z' \in H(a)$ then $x \leq x'$ or $z \leq z'$.

Note that this holds if and only if $\phi(a) \notin \Delta_x H(a)\Delta_z^{-1}$, where for any left-interval y, Δ_y is the left-closed set $\{y' \mid y' \not\geq y\}$. So (45) can be tested in polynomial time by Propositions 23 and 24.

Let E' be the collection of all pairs $\{(v, x), (v', x')\}$ from X such that the function $\bar{f}_{v,x} \vee \bar{f}_{v',x'} = \infty$, or is finite and does not belong to $\mathcal{U}$ (possibly $(v, x) = (v', x')$).

Choose a subset Y of X such that $e \cap Y \neq \emptyset$ for each $e \in E$ and such that $e \not\subseteq Y$ for each pair $e \in E'$. This is a special case of the 2-satisfiability problem, and hence can be solved in polynomial time.

Proposition 34. *If no such Y exists, there is no feasible function.*

Proof. Suppose f is a feasible function. Then $Y := \{(v, x) \in X \mid v \in V, x \leq f(v)\}$ would have the required properties. ∎

If we find Y, define f by:

(46) $\quad f(v) := \bigvee\{\bar{f}_{v,x} \mid (v, x) \in Y\}.$

Proposition 35. *f is a feasible function.*

Proof. Since $\bar{f}_{v,x} \vee \bar{f}_{v',x'} < \infty$ for each pair $\{(v, x), (v', x')\} \subseteq Y$, $f < \infty$. Moreover, f is the join of a finite number of pre-feasible functions, and hence f is pre-feasible. So by Proposition 25 it suffices to show that for each arc $a = (u, w)$:

(47) (i) there exist $x \geq f(u)$ and $z \geq f(w)$ such that $x^{-1}\phi(a)z \in H(a)$;
(ii) there exist $x \leq f(u)$ and $z \leq f(w)$ such that $x^{-1}\phi(a)z \in H(a)$.

To see (47)(i), note that it is equivalent to: $f \in \mathcal{U}$. As $\bar{f}_{v,x} \vee \bar{f}_{v',x'} \in \mathcal{U}$ for all

$(v, x), (v', x') \in Y$, Proposition 33 gives $f \in \mathcal{U}$.

To see (47)(ii), note that it is equivalent to:

$$\text{(48)} \qquad \phi(a) \in H^{\downarrow}_{f(u)} H(a) (H^{\downarrow}_{f(w)})^{-1}.$$

Suppose (48) does not hold. Let b be the largest element in $H^{\downarrow}_{f(u)} H(a)$ satisfying $b \le \phi(a)$. So by Proposition 23, $b^{-1}\phi(a) \notin (H^{\downarrow}_{f(w)})^{-1}$; that is, $\phi(a^{-1})b \not\le f(w)$. Hence there exists a left-interval z of $\phi(a^{-1})b$ such that $z \not\le f(w)$. So $\phi(a^{-1})b \notin \Delta_z$ and hence by Proposition 23, $\phi(a) \notin H^{\downarrow}_{f(u)} H \Delta_z^{-1}$. Note that since $b \le \phi(a)$ and $z \le \phi(a^{-1})b$ we have $z \le \phi(a^{-1})$ and hence $(w, z) \in X$.

Let c be the largest element in $\Delta_z H^{-1}$ such that $c \le \phi(a^{-1})$. By Proposition 23, $\phi(a)c \notin H^{\downarrow}_{f(u)}$; that is $\phi(a)c \not\le f(u)$. Hence there exists a left-interval x of $\phi(a)c$ such that $x \not\le f(u)$. Again, since $c \le \phi(a^{-1})$ and $x \le \phi(a)c$ we have $x \le \phi(a)$ and hence $(u, x) \in X$. So $\phi(a)c^{-1} \notin \Delta_x$ and hence by Proposition 23, $\phi(a) \notin \Delta_x H \Delta_z^{-1}$. So $\{(u, x), (w, z)\} \in E$ and hence Y contains at least one of $(u, x), (w, z)$. So $x \le f(u)$ or $z \le f(w)$, a contradiction. ∎

Thus we have proved:

Theorem 2. *The cohomology feasibility problem for free partially commutative groups is solvable in polynomial time.* ∎

4.6. The 2-satisfiability problem

In the algorithm we use a polynomial-time algorithm for the 2-satisfiability problem. Conversely, the 2-satisfiability problem can be seen as a special case of the cohomology feasibility problem for free groups. To see this, first note that any instance of the 2-satisfiability problem can be described as one of solving a system of inequalities in $\{0, 1\}$ variables $x_1, \ldots, x_n$ of the form:

$$\text{(49)} \qquad \begin{aligned} &x_i + x_j \ge 1 \text{ for each } \{i, j\} \in E, \\ &x_i + x_j \le 1 \text{ for each } \{i, j\} \in E', \end{aligned}$$

where E and E' are given collections of pairs and singletons from $\{1, \ldots, n\}$. (So we allow $i = j$ in (49), yielding $2x_i \ge 1$ or $2x_i \le 1$.)

Let G be the free group generated by the elements g and h. Make a directed graph with vertices $v_1, \ldots, v_n$ and with arcs:

(50) (i) $a = (v_i, v_j)$, with $\phi(a) := ghg^{-1}$, for each $\{i, j\} \in E$;
(ii) $a = (v_i, v_j)$, with $\phi(a) := h$, for each $\{i, j\} \in E'$.

Moreover, set $H(a) := \{w \in G \mid |w| \le 2\}$ for each arc a.

Now the cohomology feasibility problem in this case is equivalent to solving (49) in $\{0, 1\}$ variables. Indeed, if $x_1, \ldots, x_n$ is a solution of (49) then define $p(v_i) := g$ if $x_i = 1$

and $p(v_i) := 1$ if $x_i = 0$. Then p is a feasible function. Conversely, if p is a feasible function, define $x_i := 1$ if $p(v_i) \neq 1$ and the first symbol of $p(v_i)$ is equal to g, and $x_i := 0$ otherwise. Then $x_1, \ldots, x_n$ is a solution of (49).

4.7. A good characterization

One may derive from the algorithm a 'good' characterization of the feasibility of the cohomology feasibility problem for free partially commutative groups, i.e., one showing that the problem belongs to NP∩co-NP. We use the following well-known characterization for the feasibility of (49). Assume that for all $h, i, j, k \in \{1, \ldots, n\}$:

(51) if $\{h,i\} \in E', \{i,j\} \in E, \{j,k\} \in E'$ then $\{h,k\} \in E'$.

(Extending iteratively E' by any such pair $\{h,k\}$ does not change the set of solutions of (49).)

Then (49) has a $\{0,1\}$ solution if and only if

(52) there is no $\{i,j\} \in E$ such that both $\{i\}$ and $\{j\}$ belong to E'.

(If (51) does not hold, we could describe this condition in terms of pairs of 'alternating' cycles in $E \cup E'$. If we would require moreover that (51) holds with E and E' interchanged, the condition will be that $E \cap E'$ does not contain any singleton.)

We may adapt the subroutine in such a way that for each input $D = (V, A), \phi : A \to G, H(a)$ $(a \in A)$, and $f : V \to G$, we have as output:

(53)
(i) function $\bar{f} < \infty$, or
(ii) a cycle C violating (25), or
(iii) vertices u, v, w of D, a directed $u - v$ path P and a directed $w - v$ path Q such that $\beta_P(f(u)) \vee \beta_Q(f(w)) = \infty$.

Theorem 3. *Let be given a directed graph $D = (V, A)$, a free partially commutative group G, a function $\phi : A \to G$, and for each arc a, a closed subset $H(a)$ of G. Then there exists a function $\psi : A \to G$ such that ψ is cohomologous to ϕ and $\psi(a) \in H(a)$ for each arc a, if and only if*

(54) *for each vertex u and each two $u - u$ paths P, Q there exists an $x \in G$ such that $x^{-1} \cdot \phi(P) \cdot x \in H(P)$ and $x^{-1} \cdot \phi(Q) \cdot x \in H(Q)$.*

Proof. Necessity. Let f be a feasible function. Then for $x := f(u)$ we have $x^{-1} \cdot \phi(P) \cdot x \in H(P)$ and $x^{-1} \cdot \phi(Q) \cdot x \in H(Q)$.

Sufficiency. Let (54) be satisfied, and assume that there is no feasible function f; that is, by Section 5. Note that (54) implies (25).

Let X, E and E' be defined as in Section 5. We first show that E and E' satisfy (51). Let $\{(s,w),(t,x)\} \in E', \{(t,x),(u,y)\} \in E, \{(u,y),(v,z)\} \in E'$. Assume $\{(s,w),(v,z)\} \notin E'$; that is, $f := \bar{f}_{s,w} \vee \bar{f}_{v,z}$ is finite and belongs to $\mathcal{U}$. By definition of E, $a = (t,u)$ is an arc, and, since $f(t)^{-1}\phi(a)f(u) \in H(a)$, $x \leq f(t)$ or $y \leq f(u)$. By symmetry we may assume $x \leq f(t)$. This implies that $f_{t,x} \leq f$. Therefore, $f_{s,w} \vee f_{t,x} \leq f$, implying $\bar{f}_{s,w} \vee \bar{f}_{t,x} \leq f$. So $\bar{f}_{s,w} \vee \bar{f}_{t,x}$ is finite and belongs to $\mathcal{U}$. This contradicts the fact that $\{(s,w),(t,x)\} \in E'$.

Since there is no feasible function, there is no subset Y of X such that $e \cap Y \neq \emptyset$ for each $e \in E$ and such that $e \not\subseteq Y$ for each $e \in E'$. As (51) is satisfied it implies that there exists an arc $a = (u,w)$ and left-intervals x, z such that $\{(u,x),(w,z)\} \in E$ and such that $\{(u,x)\}, \{(w,z)\} \in E'$. Then $x \leq \phi(a)$ and $z \leq \phi(a^{-1})$. Since $\{u,x\} \in E'$, we know that $\bar{f}_{u,x} = \infty$ or is finite and does not belong to $\mathcal{U}$. It implies that

(55) (i) there exist a vertex v and two $u-v$ paths P, P' such that $\beta_P(x) \vee \beta_{P'}(x) = \infty$, or

(ii) there exist an arc $b = (v,v')$, a $u-v$ path P and a $u-v'$ path P' such that there do not exist $y \geq \beta_P(x)$ and $y' \geq \beta_{P'}(x')$ satisfying $y^{-1}\phi(a)y \in H(a)$.

Let C be the $u-u$ cycle $P(P')^{-1}$ if (i) holds, and let C be the $u-u$ cycle $Pb(P')^{-1}$ if (ii) holds. Then

(56) there do not exist $c \geq x$ and $c' \geq x$ such that $c^{-1}\phi(C)c' \in H(C)$.

To see this, assume such c, c' do exist. Suppose first that (55)(i) holds. Since $c^{-1}\phi(C)c' \in H(C) = H(P)H(P')^{-1}$, there exists an $y \in G$ such that $h := c^{-1}\phi(P)y \in H(P)$ and $h' := (c')^{-1}\phi(P')y \in H(P')$. Hence $\beta_P(x) \leq \beta_P(c) \leq \phi(P^{-1})ch = y$, and similarly $\beta_{P'}(x) \leq y$. So $\beta_P(x) \vee \beta_{P'}(x) \leq y$, contradicting (55)(i).

Suppose next that (55)(ii) holds. Since $c^{-1}\phi(C)c' \in H(C) = H(P)H(b)H(P')^{-1}$, there exist y, y' such that $h := c^{-1}\phi(P)y \in H(P), h' := (c')^{-1}\phi(P')y' \in H(P')$ and $y^{-1}\phi(b)y' \in H(b)$. Hence $\beta_P(x) \leq \beta_P(c) \leq \phi(P^{-1})ch = y$, and similarly $\beta_{P'}(x) \leq y'$. This contradicts (55)(ii).

Similarly, there exists a $w-w$ cycle D satisfying

(57) there do not exist $d \geq z$ and $d' \geq z$ such that $d^{-1}\phi(D)d' \in H(D)$.

By (54), there exists a c such that $c^{-1}\phi(C)c \in H(C)$ and $c^{-1}\phi(aDa^{-1})c \in H(aDa^{-1})$. Hence there exist d, d' such that $c^{-1}\phi(a)d \in H(a), d^{-1}\phi(D)d' \in H(D)$ and $(d')^{-1}\phi(a^{-1})c \in H(a^{-1})$. By (56), $c \not\geq x$. Since $c^{-1}\phi(a)d \in (a)$ and $\{(u,x),(w,z)\} \in E$ we know $d \geq z$. Similarly, $d' \geq z$, contradicting (57). ∎

Remark 1. Condition (54) cannot be relaxed to requiring that for each cycle P there exists an $x \in G$ such that $x^{-1} \cdot \phi(P) \cdot x$ belongs to $H(P)$. To see this, let G be the free group generated by g and h. Let D be the directed graph with one vertex v and two loops, a and b, attached at v. Define $\phi(a) := h, H(a) := \{1, h, g, g^{-1}, g^{-1}h, hg\}$ and $\phi(b) := ghg^{-1}, H(b) := \{1, h, g, g^{-1}, hg^{-1}, gh\}$. If $x^{-1} \cdot \phi(a) \cdot x \in H(a)$ then the first symbol

of x is not equal to g. If $x^{-1} \cdot \phi(b) \cdot x^{-1} \in H(b)$ then the first symbol of x is equal to g. So there is no x such that both hold.

On the other hand, for each path P there is an x such that $x^{-1} \cdot \phi(P) \cdot x \in H(P)$. Indeed, for each $k \in \mathbb{Z}$, $\phi(ab^k) \in H(ab^k)$ and $\phi(b^k a) \in H(b^k a)$. It follows that if P starts or ends with a or a^{-1}, then $\phi(P) \in H(P)$. Moreover, for each $k \in \mathbb{Z}$, $g^{-1} \cdot \phi(a^k b) \cdot g \in H(a^k b)$ and $g^{-1} \cdot \phi(ba^k) \cdot g \in H(ba^k)$. So if P starts and ends with b or b^{-1} then $g^{-1} \cdot \phi(P) \cdot g \in H(P)$. ∎

The fact that Theorem 3 is a good characterization relies on the facts that if the cohomology feasibility problem for free partially commutative groups has a solution, it has one of small size, and that if paths P, Q violating (54) would exist, there are such paths of polynomial length. (Both facts follow from the polynomial-time solvability of the subroutine.) We can check in polynomial time whether or not for given $u-u$ paths P and Q there exists an $x \in G$ such that $x \cdot \phi(P) \cdot x^{-1}$ belongs to $H(P)$ and $x \cdot \phi(Q) \cdot x^{-1}$ belongs to $\phi(Q)$. (By the closedness of $H(P)$ and $H(Q)$ we have to consider for x only beginning segments of $\phi(P), \phi(P)^{-1}, \phi(Q), \phi(Q)^{-1}$. The number of such candidates for x is polynomially bounded.)

4.8. *R*-cohomologous functions

In order to obtain results about paths instead of circuits, we extend the notion of cohomologous functions to 'R-cohomologous' functions. Again, let $D = (V, A)$ be a directed graph, and let $(G, \cdot)$ be a group. Moreover, let $R \subseteq V$. Then two functions $\phi, \psi : A \to G$ are called *R-cohomologous* if there exists a function $p : V \to G$ such that

(58) (i) $p(v) = \emptyset$ for all $v \in R$;
(ii) $\psi(a) = p(u) \cdot \phi(a) \cdot p(w)^{-1}$ for each arc $a = (u, w)$.

Again this defines an equivalence relation.

(One easily checks that if each component of D contains at least one vertex in R, then ϕ and ψ are equivalent, if and only if $\phi(P) = \psi(P)$ for each $r-s$ path P with $r, s \in R$. If D is connected and $R = \{r\}$, there is a one-to-one correspondence between R-cohomology classes and homomorphisms $\Phi : \pi(D) \to G$, given by $\Phi(\langle P \rangle) := \phi(P)$ for any $r-r$ path P. Here $\pi(D)$ denotes the fundamental group of D with base point r, and $\langle P \rangle$ denotes the homotopy class containing path P. Note that $\pi(D)$ itself is a free group. We will not use these observations in the sequel.)

Consider the *R-cohomology feasibility problem*:

(59) given: a directed graph $D = (V, A)$, a subset R of V, a function $\phi : A \to G$, and for each $a \in A$, a subset $H(a)$ of G;
find: a function $\psi : A \to G$ such that ψ is R-cohomologous to ϕ and such that $\psi(a) \in H(a)$ for each $a \in A$.

So equivalent is finding a function $p : V \to G$ such that $p(v) = 0$ for all $v \in R$ and $p(u) \cdot \phi(a) \cdot p(w)^{-1} \in H(a)$ for each arc $a = (u, w)$.

If G is a free partially commutative group G and each $H(a)$ is closed, we can reduce problem (59) easily to the cohomology feasibility problem for free partially commutative groups. We just add a loop at each vertex $v \in R$, add a new generator g_0 to the set of generators, and define $\phi(a) := g_0$ and $H(a) := \{\emptyset, g_0\}$ for each new arc (loop) a. Let $\tilde{D}, \tilde{\phi}$ and $\tilde{C}$ denote the modified input. One easily checks that the cohomology feasibility problem for $\tilde{D}, \tilde{\phi}, \tilde{C}$ is equivalent to the R-cohomology problem for D, ϕ, C. (Indeed, any feasible potential p for $\tilde{D}, \tilde{\phi}, \tilde{C}$ should satisfy $p(v) = \emptyset$ for all $v \in R$.)

Thus we have:

Theorem 4. *The R-cohomology feasibility problem for free partially commutative groups is solvable in polynomial time.* ∎

We can also derive from Theorem 3 a good characterization:

Theorem 5. *Let be given a directed graph $D = (V, A)$, a subset R of V, a free partially commutative group G, a function $\phi : A \to G$, and for each arc a, a closed subset $H(a)$ of G. Then there exists a function $\psi : A \to G$ such that ψ is R-cohomologous to ϕ and $\psi(a) \in H(a)$ for each arc a, if and only if*

(60) (i) *for each $r - s$ path P with $r, s \in R$ one has $\phi(P) \in H(P)$;*
(ii) *for each vertex s and each two $s - s$ paths P, Q there exists an $x \in G$ such that $x \cdot \phi(P) \cdot x^{-1}$ belongs to $H(P)$ and $x \cdot \phi(Q) \cdot x^{-1}$ belongs to $H(Q)$.*

Proof. Necessity being trivial, we show sufficiency. We extend D, C, ϕ to $\tilde{D}, \tilde{C}, \tilde{\phi}$ as above. It suffices to show that (60) implies (54) (with respect to $\tilde{D}, \tilde{C}, \tilde{\phi}$).

Let P and Q be two $s - s$ paths in $\tilde{D}$, for some $s \in V$. We must show that

(61) there exists an $x \in \tilde{G}$ such that $x \cdot \tilde{\phi}(P) \cdot x^{-1} \in \tilde{C}(P)$ and $x \cdot \tilde{\phi}(Q) \cdot x^{-1} \in \tilde{C}(Q)$.

I. If P and Q do not traverse any of the new loops attached at the points in R, then (61) directly follows from (60)(ii).

II. If both P and Q traverse some of the new loops, we can write $P = P_0 a_1 P_1 \cdots a_m P_m$ and $Q = Q_0 b_1 Q_1 \cdots b_n Q_n$, where $a_1, \ldots, a_m$ and $b_1, \ldots, b_n$ are new loops, and $P_0, \ldots, P_m$ and $Q_0, \ldots, Q_n$ are paths in the original graph D.

By (60)(i), $\phi(P_i) \in H(P_i)$ for $i = 1, \ldots, m-1$ and $\phi(Q_i) \in H(Q_i)$ for $i = 1, \ldots, n-1$. Moreover, by the construction of $\tilde{D}, \tilde{C}, \tilde{\phi}$, one has that $\tilde{\phi}(a_i) \in \tilde{C}(a_i)$ for $i = 1, \ldots, m$ and $\tilde{\phi}(b_i) \in \tilde{C}(b_i)$ for $i = 1, \ldots, n$.

Consider the 'surpluses' $\sigma(P_0^{-1}), \sigma(P_m), \sigma(Q_0^{-1}), \sigma(Q_n)$. Let x be one of largest size. We show that

(62) $\phi(T) \cdot x^{-1} \in H(T)$ for each $T \in \{P_0^{-1}, P_m, Q_0^{-1}, Q_n\}$.

Without loss of generality, $x = \sigma(P_0^{-1})$. Let $y := \beta(P_0^{-1})$. So $\phi(P_0^{-1}) = yx$. If x is an end segment of $\phi(T)$, then trivially $\sigma(T)$ is end segment of$x$ (as x is at least as large as x),

and hence $\phi(T) \cdot x^{-1}$ belongs to $H(T)$. If x is not an end segment of $\phi(T)$ then the last symbol of $\phi(T) \cdot x^{-1}$ is equal to the last symbol of x^{-1}. So $\phi(T) \cdot \phi(P_0) = \phi(T) \cdot (x^{-1}y^{-1}) = \phi(T) \cdot x^{-1})y^{-1}$ belongs to $H(T) \cdot H(P_0)$ (since TP_0 is an $r - r'$ path with $r, r' \in R$). As by definition y is the largest beginning segment of $\phi(P_0^{-1})$ that belongs to $H(P_0^{-1})$, it follows that $\phi(T) \cdot x^{-1}$ must belong to $H(T)$. This proves (62).

It implies that $x \cdot \tilde{\phi}(P) \cdot x^{-1} = (x \cdot \phi(P_0)) \cdot \tilde{\phi}(a_1) \cdot \phi(P_1) \cdot \cdots \cdot \tilde{\phi}(a_m) \cdot (\phi(P_m) \cdot x^{-1})$ belongs to $H(P_0) \cdot H(a_0) \cdot H(P_1) \cdot \cdots \cdot H(a_m) \cdot H(P_m) = H(P)$. Similarly for Q, thus proving (61).

III. If only one of P and Q traverses some of the new loops, we may assume that P does so. Write $P = P_0 a_1 P_1 \cdots a_m P_m$ such that $a_1, \ldots, a_m$ are new loops and $P_0, P_1, \ldots, P_m$ are paths in D. As in part II one shows that there exists an $x \in G$ such that $x \cdot \phi(P_0) \in H(P_0)$ and $\phi(P_m) \cdot x^{-1} \in H(P_m)$. We may assume that $x = \emptyset$, i.e., $\phi(P_0) \in H(P_0)$ and $\phi(P_m) \in H(P_m)$. (We can reset $\phi(a) := x \cdot \phi(a)$ for each arc a with tail s and $\phi(a) := \phi(a) \cdot x^{-1}$ for each arc a with head s.)

By (60)(ii), there exists a beginning segment u of $\phi(Q)$ such that $u^{-1} \cdot \phi(Q) \cdot u$ belongs to $H(Q)$. If both $\phi(P_0^{-1}) \cdot u \in H(P_0^{-1})$ and $\phi(P_m) \cdot u \in H(P_m)$, then as in part II, $u^{-1} \cdot \phi(P) \cdot u \in H(P)$, and we have (61). So we may assume that this is not the case. Hence the largest beginning segment y of $\phi(Q)$ such that both $\phi(P_0^{-1}) \cdot y \in H(P_0^{-1})$ and $\phi(P_m) \cdot y \in H(P_m)$, satisfies $y \neq \phi(Q)$. Similarly, we may assume that the largest beginning segment z of $\phi(Q)^{-1}$ such that both $\phi(P_0^{-1}) \cdot z \in H(P_0^{-1})$ and $\phi(P_m) \cdot z \in H(P_m)$, satisfies $z \neq \phi(Q)^{-1}$.

By definition of y and z we can choose $T, U \in \{P_0^{-1}, P_m\}$ such that y is the largest beginning segment of $\phi(Q)$ with $\phi(T) \cdot y \in H(T)$ and z is the largest beginning segment of $\phi(Q)^{-1}$ with $\phi(U) \cdot z \in H(U)$.

We may assume that $z = \emptyset$. (We can reset $\phi(a) := z \cdot \phi(a)$ for each arc s with tail a and $\phi(a) := \phi(a) \cdot z^{-1}$ for each arc with head s.)

First assume $y = \emptyset$. Then $\phi(TQU^{-1}) = \phi(T)\phi(Q)\phi(U)^{-1}$. (Note that $\phi(T) \cdot \phi(Q) = \phi(T)\phi(Q)$ since $\phi(T) \in H(T)$ and $y = \emptyset$ is the largest beginning segment of $\phi(Q)$ with $\phi(T) \cdot y \in H(T)$. Similarly, $\phi(Q) \cdot \phi(U)^{-1} = \phi(Q)\phi(U)^{-1}$.) Since $\phi(TQU^{-1})$ belongs to $H(TQU^{-1})$ by (60)(i), it follows that $\phi(Q)$ belongs to $H(Q)$. So we can take $x = \emptyset$ in (61).

Next assume $y \neq \emptyset$. Then $\phi(Q)$ and $\phi(Q)^{-1}$ do not have any nonempty common beginning segment. (Otherwise there is a nonempty common beginning segment y' of y and $\phi(Q)^{-1}$. Then $\phi(U) \cdot y' \in H(U)$, contradicting the fact that $z = \emptyset$ is the largest beginning segment of $\phi(Q)^{-1}$ satisfying $\phi(U) \cdot z \in H(U)$.)

Now let $t := |y|$ and let $y_0, \ldots, y_t$ be all beginning segments of y, with $|y_i| = i$ for $i = 0, \ldots, t$. Note that for each $i = 0, \ldots, t$ one has

(63) $$\phi(P_m) \cdot y_i \in H(P_m).$$

This follows from the fact that $\phi(P_m) \cdot y_i$ is a beginning segment of at least one of $\phi(P_m)$ and $\phi(P_m) \cdot y$, where both belong to $H(P_m)$. Similarly,

(64) $$\phi(P_0^{-1}) \cdot y_i \in H(P_0^{-1}).$$

As in part II of this proof, (63) and (64) imply

(65) $\qquad y_i^{-1} \cdot \phi(P) \cdot y_i \in H(P)$ for each $i = 0, \ldots, t$.

We show that for at least one $i \in \{0, \ldots, t\}$ one has

(66) $\qquad y_i^{-1} \cdot \phi(Q) \cdot y_i$ belongs to $H(Q)$.

Combining this with (65) gives (61).

Suppose (66) does not hold. Let $z_i := y_i^{-1} \cdot \phi(Q) y_{i-1}$ for $i = 1, \ldots, t$. Then

(67) $\qquad \phi(TQ^{t+1}U^{-1}) = (\phi(T) \cdot y) z_t z_{t-1} \cdots z_2 z_1 \phi(Q) \phi(U)^{-1}$

(i.e., no cancellations except at the $\cdot$; this follows from the facts that $z = \emptyset$, that $\phi(Q)$ and $\phi(Q)^{-1}$ have no nonempty common beginning segment, and that y is the largest beginning segment of $\phi(Q)$ such that $\phi(T) \cdot y$ belongs to $H(T)$).

Then the assumption that (66) does not hold for any $i = 0, \ldots, t$ implies that $\phi(TQ^{t+1}U^{-1})$ does not belong to $H(TQ^{t+1}U^{-1})$, contradicting (60)(i). ∎

5. Directed graphs on surfaces and homologous functions

5.1. Directed graphs on surfaces and homologous functions

An embedding of a directed graph $D = (V, A)$ in a compact orientable surface S (with each face being an open disk), can be described by a collection of cycles ('faces') $C_1, \ldots, C_f$ such that for each arc a of D, each of a and a^{-1} occurs exactly once in $C_1, \ldots, C_f$. For our purposes, such a cycle collection is enough to perform the algorithms below. (We assume that each face is an open disk, which assumption does not restrict the generality of our results.)

We can think of the cycles $C_1, \ldots, C_f$ as giving the *clockwise* orientation of the faces. In this interpretation, the face that traverses a in forward direction is at the right-hand side of a, and the face that traverses a in backward direction is at the left-hand side of a.

Note that by Euler's formula, $|V| + f = |A| + 2 - 2h$, where h is the number of handles of the surface. Below when fixing a surface, we in fact just fix h.

For any directed graph$D = (V, A)$ embedded on a compact orientable surface, the *dual* graph $D^* = (\mathcal{F}, A^*)$ has vertex set the collection $\mathcal{F}$ of faces of D, while for any arc a of D there is an arc a^* of D^* with as tail the face of D at the right-hand side of a and as head the face of D at the left hand side. We define for any function ϕ on A the function ϕ^* on A^* by $\phi^*(a^*) := \phi(a)$ for each $a \in A$.

If a directed graph $D = (V, A)$ is embedded on a compact orientable surface S, we can dualize the concept of cohomologous functions to 'homologous' functions.

Denote by $\mathcal{F}$ the collection of faces of D. Let $(G, \cdot)$ be a group. We call two function $\phi, \psi : A \to G$ *homologous* if there exists a function $p : \mathcal{F} \to G$ such that for each arc a we have $p(F) \cdot \phi(a) \cdot p(F')^{-1} = \psi(a)$, where F and F' are the faces at the right-hand side and left-hand side of a, respectively.

The relation to cohomology is direct: ϕ and ψ are homologous (in D), if and only if ϕ^* and ψ^* are cohomologous (in D^*).

It follows that the *homology feasibility problem*:

(68) given: a directed graph $D = (V, A)$ embedded on a compact orientable surface S, a function $\phi : A \to G$, and for each $a \in A$, a subset $H(a)$ of G;
find: a function $\psi : A \to G$ such that ψ is homologous to ϕ and such that $\psi(a) \in H(a)$ for each $a \in A$,

is solvable in polynomial time if G is a free partially commutative group and each $H(a)$ is closed.

5.2. Circulations and cycle decompositions

Let $D = (V, A)$ be a directed graph embedded on a compact orientable surface S, and let $(G, \cdot)$ be a group. We call a function $\phi : A \to G$ a *circulation* if for each vertex v of D we have

$$(69) \qquad \phi(a_1)^{\varepsilon(v,a_1)} \cdot \ldots \cdot \phi(a_m)^{\varepsilon(v,a_m)} = 1$$

where $a_1, \ldots, a_m$ are the arcs incident with v, in clockwise order, and $\varepsilon(v, a_i) := +1$ if a_i enters v, and $:= -1$ if a_i leaves v. (If a_i is a loop at v we should be more careful.)

So ϕ is a circulation, if and only if for each cycle π bounding a face of D^* one has $\phi^*(\pi) = 1$. Note that in this last characterization it is not necessary to restrict oneself to clockwise cycles. Consider e.g. three arcs, a, b, c entering v, in clockwise order, with $\phi(a) \cdot \phi(b) \cdot \phi(c) = 1$. Then $\phi(c) \cdot \phi(b) \cdot \phi(a)$ is generally not equal to 1. However, for $\pi := a^*b^*c^*$, both $\phi^*(\pi)$ and $\phi^*(\pi^{-1})$ are equal to 1.

It is easy to check that if ϕ is a circulation and ψ is homologous to ϕ, then ψ is again a circulation.

If G is a free group, any circulation $\phi : A \to G$ can be decomposed as follows. Replace any arc a of D by $t := |\phi(a)|$ parallel arcs $a_1, \ldots, a_t$ (from right to left), yielding the graph $D_\phi = (V, A_\phi)$. Define $\phi'(a_i) := \xi_i$, where ξ_i is the ith symbol in $\phi(a)$, for $i = 1, \ldots, t$.

Consider now any vertex v. Since (69) holds we can find a perfect matching on the arcs of D_ϕ incident with v (more precisely, on $\{1, \ldots, m\}$) in such a way that:

(70) (i) for any matched pair $\{a, b\}$ we have $\phi'(a)^{\varepsilon(v,a)} = \phi'(b)^{-\varepsilon(v,b)}$;
(ii) if $\{a, b\}$ and $\{c, d\}$ are matched pairs, thenthe path $a^{-\varepsilon(v,a)}b^{\varepsilon(v,b)}$ does not cross the path $c^{-\varepsilon(v,c)}d^{\varepsilon(v,d)}$ at v.

Combining all matched pairs, at all vertices, we obtain a decomposition of A_ϕ into a collection $\mathcal{C}$ of cycles, which we call a *cycle decomposition* of ϕ. The cycles do not have any fixed end point (formally speaking, we identify all cyclic permutations of the cycle). No cycle in $\mathcal{C}$ crosses itself or any of the other cycles in $\mathcal{C}$.

Each cycle C in $\mathcal{C}$ has associated with it a symbol $\xi(C)$ from $g_1, g_1^{-1}, g_2, g_2^{-1}, \ldots$, such that for each arc a of D_ϕ, if C traverses a in forward direction then $\phi'(a) = \xi(C)$ and if C traverses a in backward direction then $\phi'(a) = \xi(C)^{-1}$. The collection $\mathcal{C}$ together with the function $\xi : \mathcal{C} \to \{g_1, g_1^{-1}, g_2, g_2^{-1}, \ldots, \}$ uniquely determine ϕ (but generally not conversely).

We may consider the cycles in $\mathcal{C}$ as cycles in D (rather than in D_ϕ) if, for each arc a of D, we keep track of the order (from right to left) in which the cycles in $\mathcal{C}$ traverse a.

5.3. Disjoint circulations

Let $D = (V, A)$ be a directed graph embedded on a compact orientable surface. We call a circulation $\phi : A \to G_\infty$ *simple and directed* if any cycle decomposition of ϕ consists of pairwise vertex-disjoint simple directed cycles. (A cycle is *simple* if no vertex is traversed more than once (except for the end vertices). A cycle is *directed* if it does not contain a^{-1} for any arc a.)

Consider the problem:

(71) given: a directed graph $D = (V, A)$ embedded on a compact orientable surface S and a circulation $\phi : A \to G_\infty$;
find: a simple and directed circulation ψ homologous to ϕ.

In order to show that this problem is solvable in polynomial time, we define for each directed graph D embedded on a compact orientable surface S, the 'extended' dual graph $D^+ = (\mathcal{F}, A^+)$ as the graph obtained from D^* by adding in each face of D^* all chords. (So generally D^+ is not embeddable in S.) More precisely, for each nonempty path π on the boundary of any face of D^*, D^+ has an arc a_π; if π is an $F - F'$ path, a_π runs from F to F'. (Since each arc a^* is such a path, D^+ contains D^* as a subgraph.)

For any $\phi : A \to G$, where G is a group, define $\phi^+ : A^+ \to G$ by $\phi^+(a_\pi) := \phi^*(\pi)$ for each $a_\pi \in A^+$.

Theorem 6. *Problem* (71) *is solvable in polynomial time.*

Proof. Define

$$
\begin{aligned}
(72)\qquad & H(a_\pi) := \{1, g_1, g_2, \ldots\} \text{ if } \pi := a^* \text{ for any arc } a^* \text{ of } D^*, \\
& H(a_\pi) := \{1, g_1, g_1^{-1}, g_2, g_2^{-1}, \ldots\} \text{ for all other arcs } a_\pi \text{ of } D^+.
\end{aligned}
$$

By Theorem 2 we can find in polynomial time a function $\vartheta : A^+ \to G_\infty$ such that ϑ is cohomologous to ϕ^+ and such that $\vartheta(a_\pi) \in H(a_\pi)$ for each arc a_π of D^+. Defining $\psi(a) := \vartheta(a^*)$ for each $a \in A$ gives a solution of (71).

Moreover, if (71) has a solution ψ, then such a function ϑ exists, viz. $\vartheta := \psi^+$, as one directly checks. ∎

5.4. The torus

Theorem 3 implies a good characterization for the feasibility of (71), in terms of closed curves on S. It is related to the one given in [11], where for any undirected graph G embedded on a compact surface S and any set of pairwise disjoint simple closed curves $C_1, \ldots, C_k$ on S, it was characterized when there exist pairwise disjoint simple circuits $C'_1, \ldots, C'_k$ in G such that C'_i is freely homotopic to C_i for $i = 1, \ldots, k$. (Freely homotopic means that there is no 'base point'.) However, in the present paper we consider the homology relation, which

is coarser than homotopy, and so the two characterization do not seem to follow from each other.

However, if S is the torus, the two concepts coincide. This case has been dealt with by Seymour Seymour [14] (cf. Ding, Schrijver, and Seymour [3]).

Let $S = S^1 \times S^1$ be the torus, where S^1 is a closed curve. Let S_1 be the closed curve $S^1 \times \{1\}$ on S (fixing some orientation). Let $C_1, \ldots, C_k$ be pairwise disjoint simple closed curves on S, each being freely homotopic to S_1 or to S_1^{-1}, choosing indices such that $C_1, \ldots, C_k$ occur cyclically around the torus (when going from the left-hand side of S_1 to the right-hand side). We let the *sign* of $C_1, \ldots, C_k$ to be the vector $x \in \{+1, -1\}^k$ where $x_i = +1$ if C_i is freely homotopic to S_1, and $x_i := -1$ if C_i is freely homotopic to S_1^{-1}.

For each closed curve L on S let the *winding number* $w(L)$ be equal to the number of times L crosses S_1 from right to left, minus the number of times L crosses S_1 from left to right.

Let $D = (V, A)$ be a directed graph embedded on the torus S, and let L be a closed curve on S with $w(L) \geq 0$. We say that L *fits* $x \in \{+1, -1\}^k$ if L traverses points $p_1, \ldots, p_{kw(L)}$, in this order, such that for each $j = 1, \ldots, kw(L)$:

(73) either (i) $p_j \in V$,
or (ii) p_j is on some arc a of D such that D crosses a from right to left if $x_j = +1$, and D crosses a from left to right if $x_j = -1$,

taking indices of x_j modulo k. We derive the following theorem of Seymour [14]:

Theorem 7. *Let $D = (V, A)$ be a directed graph embedded on the torus S and let $x \in \{+1, -1\}^k$. Then D contains pairwise disjoint simple directed circuits each being freely homotopic to S_1 or S_1^{-1}, with sign x, if and only if*

(74) *each closed curve L on S fits some cyclic permutation of x.*

Proof. Necessity being trivial, we show sufficiency. Let $k \geq 1$ and let (74) be satisfied. This easily implies that D has at least one (undirected) circuit C that is a freely homotopic to S_1. Let G be the free group generated by $g_1, \ldots, g_k$ and let $z := g_1^{x_1} \cdots g_k^{x_k}$. Define for each arc a of D, $\phi(a) := z$ if a that is traversed by C in forward direction, $\phi(a) := z^{-1}$ if a that is traversed by C in backward direction, and $\phi(a) := 1$ otherwise. Let $H(a_\pi)$ be as in (72).) Each path P in D^+ corresponds in a natural way to a curve on S which we also denote by P.

We show that for each face F and any two $F - F$ paths P, Q in D^+ there exists an $x \in G$ such that

(75) $$x \cdot \phi^+(P) \cdot x^{-1} \in H(P) \text{ and } x \cdot \phi^+(Q) \cdot x^{-1} \in H(Q).$$

We may assume that $w(P) \geq 0$ and $w(Q) \geq 0$. Note that $\phi^+(P) = z^{w(P)}$ and $\phi^+(Q) = z^{w(Q)}$. Assume that such an x does not exist. Define $z_i := g_{i+1}^{x_{i+1}} \cdots g_k^{x_k}$, for $i = 0, \ldots, k$. By assumption, for each $i = 1, \ldots, k$ there exists an $R_i \in \{P, Q\}$ such that $z_i \cdot \phi^+(R_i) \cdot z_i^{-1} \notin$

$H(R_i)$. Let $R := R_k R_{k-1} \cdots R_1 R_0$. So $w(R) = w(R_k) + \cdots + w(R_0)$ and $\phi^+(R) = z^{w(R)}$. By (74), some cyclic permutation of $\phi^+(R)$ belongs to $H(R)$. Hence $z^{w(R)-1} g_1^{x_1}$ belongs to $H(R)$. Since $z^{w(R)-1} = \prod_{i=k}^{1} (z_i z^{w(R_i)} \cdot z_{i-1}^{-1})$ and $H(R) = \prod_{i=k}^{1} H(R_i)$, there exists an $i = 1, \ldots, k$ such that $z_i z^{w(R_i)} \cdot z_i^{-1}$ belongs to $H(R_i)$, a contradiction. This show that there exists an $x \in G$ satisfying (75).

Now by Theorem 9 there exists a function $\vartheta : A^+ \to G$ cohomologous to ϕ^+ such that $\vartheta(a_\pi) \in H(a_\pi)$ for each arc a_π of D^+. Define $\psi(a) := \vartheta(a_{a^*})$ for each arc a of D. Then ψ is a simple and directed circulation homologous to ϕ. Since for each cycle P in D^* one has $\psi^*(P) = \phi * (P)$ it follows that any cycle decomposition of ψ consists of directed circuits of the required type. ∎

A stronger version, also given by Seymour [14], in which we prescribe for each arc a of D which of the directed circuits $C_1, \ldots, C_k$ are permitted to traverse a, can also be derived. (To this end we restrict the $H(a_{a^*})$.)

5.5. $\mathcal{R}$-homologous function, δ-joins, and path decompositions

Dual to $\mathcal{R}$-cohomologous functions are $\mathcal{R}$-homologous functions. Let $D = (V, A)$ be a directed graph embedded on a compact orientable surface S, with face collection $\mathcal{F}$, and let $\mathcal{R} \subseteq \mathcal{F}$. Let $(G, \cdot)$ be a group. We call two functions $\phi, \psi : A \to G$ *$\mathcal{R}$-homologous* if there exists a function $p : \mathcal{F} \to G$ such that $p(F) = 1$ for each $F \in \mathcal{R}$ and such that for each arc a we have $p(F) \cdot \phi(a) \cdot p(F')^{-1} = \psi(a)$, where F and F' are the faces at the right-hand side and left-hand side of a, respectively. Again it follows that the *$\mathcal{R}$-homology feasibility problem for free partially commutative groups* is solvable in polynomial time.

An extension of the notion of circulation is the 'δ-join'. Let $\delta : V \to G$ (a 'demand function') be such that

(76) each vertex v with $\delta(v) \neq 1$ has degree one.

(That is, v is incident with exactly one arc.) Call a function $\phi : A \to G$ a *δ-join* if for each vertex v:

(77) $$\phi(a_1)^{\varepsilon(v,a_1)} \cdot \ldots \cdot \phi(a_m)^{\varepsilon(v,a_m)} = \delta(v),$$

where again $a_1, \ldots, a_m$ are the arcs incident with v in clockwise order, and for any arc a incident with v, $\varepsilon(v, a) := +1$ if a leaves v and $\varepsilon(v, a) := -1$ if a enters v. So if $\delta(v) = 1$ for each vertex v, any δ-join is a circulation.

Let W be the set of vertices v satisfying $\delta(v) \neq 1$, and let $\mathcal{R}$ be the collection of faces incident with at least one vertex in W. One directly checks:

(78) if ϕ is a δ-join and ψ is $\mathcal{R}$-homologous to ϕ, then ψ is a δ-join again.

An extension of the idea of the cycle decomposition of a circulation is that of a 'path decomposition' of a δ-join. Let G be a free group. Again we make the directed graph $D_\phi = (V, A_\phi)$. At each vertex $v \notin W$ we can find a matching as for circulations. Combining

all matched pairs we obtain a decomposition of A_ϕ into a collection $\mathcal{P}$ of paths and cycles, which we call a *path decomposition* of ϕ. Each path has tail and head in W (possibly the same vertex). The cycles do not have any given fixed end point (formally speaking, we identify all cyclic permutations of the cycle). All vertices traversed by the paths except for their ends, and all vertices traversed by the cycles, belong to $V \setminus W$. Moreover, none of the paths and cycles crosses itself or any of the other paths and cycles.

Each path and cycle P in $\mathcal{P}$ has associated with it a symbol $\xi(P)$ from $\{g_1, g_1^{-1}, g_2, g_2^{-1}, \ldots\}$, such that for each arc a of D_ϕ, if P traverses a in forward direction then $\phi'(a) = \xi(P)$ and if P traverses a in backward direction then $\phi'(a) = \xi(P)^{-1}$. The pair $\mathcal{P}, \xi$ determines ϕ.

5.6. Enumerating homology types

With the methods developed before we can find in polynomial time a δ-join of given homology type. In order to be able to consider all homology types of a certain restricted size, we describe an enumeration. (A related enumeration was given in [12].)

We call a δ-join ϕ *elementary* if ϕ has a path decomposition with paths only (all starting and ending in W). We first consider the following problem for any p and compact orientable surface S:

(79) given: a directed graph $D = (V, A)$ embedded on S, with exactly p faces, a natural number m, and a function $\delta : V \to G_\infty$ such that each vertex in the set $W := \{v \mid \delta(v) \neq 1\}$ has degree 1;
find: all elementary δ-joins ϕ with $|\phi(a)| \leq m$ for each arc a not incident with any vertex in W.

Theorem 8. *For each fixed p and compact orientable surface S, problem* (79) *is solvable in polynomial time.*

[As input size we take $|V| + |A| + m + \sum_{v \in V} |\delta(v)|$.]

Proof. We may assume that $|V \setminus W| = 1$. To see this, consider any arc a connecting two different vertices in $V \setminus W$. Let $D' = (V', A')$ arise from D by contracting a. Let $\delta'(v) := \emptyset$ for the contracted vertex v, and let δ' coincide with δ on all other vertices. Then for each δ'-join ϕ' there is a unique δ-join ϕ such that $\phi|A' = \phi'$. So any enumeration of δ'-joins gives directly an enumeration of δ-joins.

Let $V = W \cup \{u\}$ for some vertex u. Hence D consists of one vertex u, with a number of oriented loops at u, and a number of arcs connecting u with the vertices in W, each of degree one. We may assume that each of the nonloops has tail in W and head u. Let L denote the set of loops of D. By Euler's formula, $|L| = p + 2h - 1$. So when considering the arcs incident with u in clockwise order, there are $2p + 4h - 2$ (possibly empty) consecutive groups of nonloops, separated by loops. Let the jth group, W_j say, consist of the arcs $(w_{j,1}, u), \ldots, (w_{j,t_j}, u)$, in clockwise order. Let $\tilde{D}$ arise from D by identifying for each j all vertices $w_{j,1}, \ldots, w_{j,t_j}$ to one vertex w_j and identifying all parallel arcs (w_j, u) arising.

Consider any elementary δ-join with $|\phi(a)| \leq m$ for each loop a of D. Let $P_1, \ldots, P_M$ form a path decomposition of ϕ. Define the *type* of a path P_i as the path in $\tilde{D}$ obtained

from P by traversing the arcs in $\tilde{D}$ that are parallel to those in P.

Let $Q_1, \ldots, Q_K$ be all types of $P_1, \ldots, P_M$ that are different from aa^{-1} for any arc a. We identify type Q with Q^{-1}. Now ϕ is completely determined by the Q_i, together with a word y_i in G associated to Q_i (for each i) that forms the concatenation of the symbols asociated with the P_j of type Q_i (in the appropriate order).

We show that we can choose the Q_j with the associated words in a polynomially bounded number of ways (fixing p and h). First we show that K is at most $9p + 18h$. Since $P_1, \ldots, P_M$ are pairwise noncrossing, we can decouple the paths $Q_1, \ldots, Q_K$ at u, so as to obtain pairwise disjoint paths $Q'_1, \ldots, Q'_K$ (disjoint except for their end points). Since any two Q_i are different, the graph H with vertex u and arcs (loops) $Q'_1, \ldots, Q'_K$ has no faces bounded by one or two edges, except for the p original faces of D. So $3(f - p) \leq 2K$, where f denotes the number of faces of H. As $\tilde{D}$ has at most $(2p + 4h - 2) + 1$ vertices, by Euler's formula we have, $K \leq 2p + 4h - 1 + f - 2 + 2h \leq 3p + 6h + \frac{2}{3}K$. Therefore $K \leq 9p + 18h$.

For any $a, b \in L \cup L^{-1}$, let m_{ab} be the number of times ab or $b^{-1}a^{-1}$ occurs in $Q_1, \ldots, Q_K$ (counting multiplicities). Since the P_i are pairwise noncrossing, we can reconstruct $\{Q_1, \ldots, Q_K\}$ from the m_{ab} (up to reversing a path).

Now $m_{ab} \leq m$ for all a, b, since $|\phi(a)| \leq m$ for each $a \in A$. So in enumerating, we can choose for each pair $a, b \in L \cup L^{-1}$ a nonnegative integer $m_{ab} \leq m$. (Since $|L| = p + 2h - 1$, there are at most $(m+1)^{(p+2h-1)^2}$ choices.) For each choice, we try to construct $Q_1, \ldots, Q_K$ from the m_{ab}. If we fail or if $K > 9p + 18h$, we go on to the next choice of the m_{ab}. If we succeed and $K \leq 9p + 18h$, we proceed as follows.

For each $i = 1, \ldots, K$, if the first arc of Q_i equals (w_j, u), the word associated with Q_i should be equal to $\bar{x}$, where x is some segment of the word

(80) $$\delta(w_{j,1}) \cdots \delta(w_{j,t_j}).$$

Here $\bar{x}$ denotes the word obtained from x by cancelling iteratively all occurrences of $\xi\xi^{-1}$ and $\xi^{-1}\xi$. (In (80) we did not cancel occurrences of $\xi\xi^{-1}$ or $\xi^{-1}\xi$. So word (80) need not be in G_∞.)

Since $K \leq 9p + 18h$ there are at most $(\sum_{i=1}^{n} |\delta(w_i)|)^{18p+36h}$ such segments, and we can consider all choices in polynomial time. Combining all choices gives us a function on the arcs of D, that is either an elementary δ-join, or not. This way we obtain all elementary δ-joins. ∎

Consider next the following problem for any compact orientable surface S:

(81) given: a directed graph $D = (V, A)$ embedded on S, a natural number m, and a function $\delta : V \to G_\infty$, such that each vertex v in the set $W := \{v \mid \delta(v) \neq \emptyset\}$ has degree one;

find: δ-joins $\phi_1, \ldots, \phi_N$ such that each elementary δ-join ϕ with $|\phi(a)| \leq m$ for each arc not incident with W, is $\mathcal{R}$-homologous to at least one of $\phi_1, \ldots, \phi_N$, where $\mathcal{R}$ is the collection of faces incident with at least one vertex in W.

Theorem 9. *For each fixed p and compact orientable surface S, problem (81) is solvable*

in polynomial time when $|\mathcal{R}| = p$.

[Again we take as input size $|V| + |A| + m + \sum_{v\in V} |\delta(v)|$.]

Proof. Let A' denote the set of arcs not incident with any vertex in W. Delete iteratively arcs from D that are incident with at least one face not in $\mathcal{R}$. We end up with a graph $\tilde{D} = (V, \tilde{A})$ that has p faces, and such that each elementary δ-join in D with $|\phi(a)| \leq m$ for each arc $a \in A'$, is $\mathcal{R}$-homologous to some elementary δ-join in $\tilde{D}$ with $|\phi(a)| \leq 2m|A|$ for each arc $a \in A'$. Thus Theorem 8 implies the required enumeration. ∎

5.7. Applications to disjoint paths and trees problems

We apply the techniques described above to a number of disjoint paths and disjoint trees problems.

We first consider the following problem, for any fixed compact surface S and any fixed p:

(82) given: a directed graph $D = (V, A)$ embedded on S and pairs $(r_1, s_1), \ldots, (r_k, s_k)$ of vertices of D, with the property that there exist p faces such that each of $r_1, s_1, \ldots, r_k, s_k$ is incident with at least one of these faces;
find: pairwise vertex-disjoint paths $P_1, \ldots, P_k$, where P_i is an $r_i - s_i$ path ($i = 1, \ldots, k$).

Theorem 10. *For each fixed compact orientable surface S and each fixed p, problem* (82) *is solvable in polynomial time.*

Proof. We may assume that $r_1, s_1, \ldots, r_k, s_k$ all are distinct and have degree one. Let $\mathcal{R}$ be the collection of faces incident with at least one of $r_1, s_1, \ldots, r_k, s_k$. Define $\delta(r_i) := g_i$ and $\delta(s_i) := g_i^{-1}$ for $i = 1, \ldots, k$. Moreover, define $\delta(v) := \emptyset$ for all other vertices v.

By Theorem 9 we can find in polynomial time (fixing S and p) a list of δ-joins $\phi_1, \ldots, \phi_N$ in D such that each elementary δ-join ϕ with $|\phi(a)| \leq 1$ for each arc a not incident with $r_1, s_1, \ldots, r_k, s_k$, is $\mathcal{R}$-homologous to at least one of the ϕ_i.

Consider the extended dual graph D^+ of D (cf. Section 3). Define for each arc a_π of D^+:

(83)
$$H(a_\pi) := \{\emptyset, g_1, \ldots, g_k\} \text{ if } \pi = a^* \text{ for some } a \in A;$$
$$H(a_\pi) := \{\emptyset, g_1, g_1^{-1}, \ldots, g_k, g_k^{-1}\} \text{ for all other } a_\pi\ .$$

By Theorem (2) we can find in polynomial time a function ϑ that is $\mathcal{R}$-cohomologous to ϕ_i^+ in D^+, with $\vartheta(b) \in H(b)$ for each arc b of D^+, provided that such a ϑ exists. If we find one, define $\psi(a) := \vartheta(a^*)$, for each arc a of D. Then ψ is a δ-join in D (as it is $\mathcal{R}$-homologous to ϕ_i), and any path decomposition of ψ into paths of cycles contains pairwise disjoint paths $P_1, \ldots, P_k$ as required.

If for none of $i = 1, \ldots, N$ we find such a ϑ we may conclude that problem (82) has no solution. For suppose $P_1, \ldots, P_k$ is a solution. Define $\phi(a) := g_i$ if P_i traverses a ($i = 1, \ldots, k$) and $\phi(a) := 1$ if a is not traversed by any $P_1, \ldots, P_k$. Since ϕ is an elementary

δ-join with $|\phi(a)| \leq 1$ for each arc a, there exists an $i \in \{1, \ldots, N\}$ such that ϕ and ϕ_i are $\mathcal{R}$-homologous. However, for this i, there exists a ϑ as above, viz. $\vartheta := \phi^+$. This contradicts our assumption. ∎

A special case applies to (1):

Corollary 10a. *For each fixed k, the k disjoint paths problem for directed planar graphs is solvable in polynomial time.*

Proof. Directly from Theorem 10. ∎

An extension of Theorem 10 applies to the following problem:

(84) given: a directed graph $D = (V, A)$ embedded on S and pairs $(r_1, S_1), \ldots, (r_k, S_k)$ with $r_1, \ldots, r_k \in V$ and $S_1, \ldots, S_k \subseteq V$, with the property that there exist p faces such that each vertex in $\{r_1, \ldots, r_k\} \cup S_1 \cup \cdots \cup S_k$ is incident with at least one of the faces;
find: pairwise vertex-disjoint rooted trees $T_1, \ldots, T_k$, where T_i has root r_i and covers S_i $(i = 1, \ldots, k)$.

Theorem 11. *For each fixed compact orientable surface S and each fixed p, problem* (84) *is solvable in polynomial time.*

Proof. We may assume that all vertices in $W := \{r_1, \ldots, r_k\} \cup S_1 \cup \cdots \cup S_k$ are distinct and have degree one. Let $\mathcal{R}$ be the collection of faces incident with at least one vertex in W. Define $\delta(r_i) := g_i^{|S_i|}$ and $\delta(s) := g_i^{-1}$ for $s \in S_i$, for $i = 1, \ldots, k$. Moreover, define $\delta(v) := 1$ for all other vertices v.

By Theorem 9 we can find in polynomial time (fixing S and p) a list of δ-joins $\phi_1, \ldots, \phi_N$ in D such that each elementary δ-join ϕ with $|\phi(a)| \leq |V|$ for each arc a not incident with $r_1, s_1, \ldots, r_k, s_k$, is $\mathcal{R}$-homologous to at least one of the ϕ_i.

Again consider the extended dual graph D^+ of D. Define for each arc a_π of D^+:

(85) $H(a_\pi) := \{g_i^n \mid i = 1, \ldots, k; n \in \mathbb{Z}, n \geq 0\}$ if $\pi = a^*$ for some $a \in A$;
$H(a_\pi) := \{g_i^n \mid i = 1, \ldots, k; n \in \mathbb{Z}\}$ for all other a_π.

By Theorem (2) we can find in polynomial time a function ϑ that is $\mathcal{R}$-cohomologous to ϕ_i^+ in D^+, with $\vartheta(b) \in H(b)$ for each arc b of D^+, provided that such a ϑ exists. If we find one, define $\psi(a) := \vartheta(a^*)$, for each arc a of D. Then ψ is a δ-join in D (as it is $\mathcal{R}$-homologous to ϕ_i), and any path decomposition of ψ into paths and cycles contains pairwise disjoint rooted trees $T_1, \ldots, T_k$ as required.

If for none of $i = 1, \ldots, N$ we find such a ϑ we may conclude that problem (84) has no solution. For suppose $T_1, \ldots, T_k$ is a solution. Define $\phi(a) := g_i^l$ if T_i contains a and for l vertices s in S_i the simple $r - s_i$ path in T_i traverses a, and $\phi(a) := 1$ if a is not contained in any $T_1, \ldots, T_k$. Since ϕ is an elementary δ-join with $|\phi(a)| \leq |V|$ for each arc a, there exists an $i \in \{1, \ldots, N\}$ such that ϕ and ϕ_i are $\mathcal{R}$-homologous. However, for this i, there

exists a ϑ as above, viz. $\vartheta := \phi^+$. This contradicts our assumption. ∎

A further extension is to the following problem:

(86) given: a directed graph $D = (V, A)$ embedded on S, subsets $A_1, \ldots, A_k$ of A, and pairs $(r_1, S_1), \ldots, (r_k, S_k)$ with $r_1, \ldots, r_k \in V$ and $S_1, \ldots, S_k \subseteq V$, with the property that there exist p faces such that each vertex in $\{r_1, \ldots, r_k\} \cup S_1 \cup \cdots \cup S_k$ is incident with at least one of these faces;
find: pairwise vertex-disjoint rooted trees $T_1, \ldots, T_k$, where T_i has root r_i, covers S_i and contains arcs only in A_i $(i = 1, \ldots, k)$.

Theorem 12. *For each fixed compact orientable surface S and each fixed p, problem* (86) *is solvable in polynomial time.*

Proof. As before, now replacing the first line in (85) by: $H(a_\pi) := \{g_i^n \mid i = 1, \ldots, k, a \in A_i; n \in \mathbb{Z}, n \geq 0\}$ if $\pi = a^*$ for $a \in A$. ∎

We do not see if our methods extend to compact *non*orientable surfaces.

5.8. Other groups and the arc-disjoint case

Our algorithms are based on the polynomial-time solvability of the cohomology feasibility problem for free groups. It might be interesting to investigate in how far the method can be extended to other groups. Especially, for which groups $(G, \cdot)$ and subsets $C \subseteq G$ is the following problem solvable in polynomial time:

(87) given: a directed graph $D = (V, A)$ and a function $\phi : A \to G$;
find: a function $\psi : A \to C$ cohomologous to ϕ.

This might apply to the arc-disjoint case as follows. It is unknown if the following problem is solvable in polynomial time or NP-complete for $k = 2$:

(88) given: a directed planar graph and vertices $r_1, s_1, \ldots, r_k, s_k$,
find: find pairwise arc-disjoint paths $P_1, \ldots, P_k$, where P_i is an $r_i - s_i$ path $(i = 1, \ldots, k)$.

If we do not require planarity the problem is NP-complete for $k = 2$, as follows from the result of Fortune, Hopcroft, and Wyllie mentioned in section 1. (The vertex-disjoint case can be reduced to the arc-disjoint case.) The complexity status of (88) is also unknown for the special case $k = 2, r_1 = s_2, s_1 = r_2$.

Now if problem (87) is polynomial-time solvable for the group $G := \mathbb{Z}^2$, taking $C = \{(0,0), (1,0), (0,1)\}$, then problem (88) is solvable in polynomial time for $k = 2$. This can be seen with a method similar to the one described in the previous sections.

More generally, if the cohomology feasibility problem for free groups is solvable in polynomial time for the group $\mathbb{Z}^k$, taking for $H(a)$ the set of all unit basis vectors together

with the origin, then problem (88) is polynomial-time solvable for this k. Note that $\mathbb{Z}^k$ can be considered as the 'free abelian group'; it is generated by $g_1, \ldots, g_k$, with relations $g_i \cdot g_j = g_j \cdot g_i$ for all $i, j = 1, \ldots, k$.

This also implies that if the group itself is part of the input of problem (87) (given, e.g., by generators and relations), then the problem will be NP-hard. This follows from the NP-completeness of problem (87) for nonfixed k. Note that the algorithm we described for the cohomology feasibility problem for free groups is polynomial-time also if we do not fix the number of generators.

In a sense there are the following correspondences:

(89)
$$\begin{aligned} \text{vertex-disjoint directed paths} &\longleftrightarrow \text{free groups,} \\ \text{arc-disjoint directed paths} &\longleftrightarrow \text{free abelian groups.} \end{aligned}$$

In the undirected case we could add the relations $g_i^2 = 1$ for $i = 1, \ldots, k$. This gives the free boolean group (all words made from $g_1, g_2, \ldots$ with no segment $g_i g_i$ for any i) and the free abelian boolean groups ($\cong \{0,1\}^k$), and the following correspondences:

(90)
$$\begin{aligned} \text{vertex-disjoint undirected paths} &\longleftrightarrow \text{free boolean groups,} \\ \text{edge-disjoint undirected paths} &\longleftrightarrow \text{free abelian boolean groups.} \end{aligned}$$

By Robertson and Seymour's result, for fixed k the k disjoint undirected paths problem is solvable in polynomial time (for the vertex-disjoint case, and hence also for the edge-disjoint case). This might suggest that problem (87) is solvable in polynomial time for any fixed free boolean (abelian) group.

However, problem (87) is NP-complete for $G := \{0,1\}^2$ and $C := \{(0,0), (1,0), (0,1)\}$, even if we fix $\phi(a) = (1,1)$ for each arc a. In that case (87) has a solution ψ if and only if D is four vertex colorable. (I thank Bert Gerards for this observation.)

References

[1] A. Baudisch, Kommutationsgleichungen in semifreien Gruppen, *Acta Mathematica Academiae Scientiarum Hungaricae* 29 (1977) 235–249.

[2] G. Birkhoff, *Lattice Theory (Third Edition)* [American Mathematical Colloquium Publications Volume XXV], American Mathematical Society, Providence, Rhode Island, 1973.

[3] G. Ding, A. Schrijver, P.D. Seymour, Disjoint paths in a planar graph — a general theorem, *SIAM Journal on Discrete Mathematics* 5 (1992) 112–116.

[4] C. Droms, Isomorphisms of graph groups, *Proceedings of the American Mathematical Society* 100 (1987) 407–408.

[5] S. Fortune, J. Hopcroft, J. Wyllie, The directed subgraph homeomorphism problem, *Theoretical Computer Science* 10 (1980) 111–121.

[6] J.F. Lynch, The equivalence of theorem proving and the interconnection problem, *(ACM) SIGDA Newsletter* 5:3 (1975) 31–36.

[7] R.C. Lyndon, P.E. Schupp, *Combinatorial Group Theory*, Springer, Berlin, 1977.

[8] W. Magnus, A. Karrass, D. Solitar, *Combinatorial Group Theory*, Wiley-Interscience, New York, 1966.

[9] B.A. Reed, N. Robertson, A. Schrijver, P.D. Seymour, Finding disjoint trees in planar graphs in linear time, in: *Graph Structure Theory* (Proceedings Joint Summer Research Conference on Graph Minors, Seattle, Washington, 1991; N. Robertson, P. Seymour, eds.) [Contemporary Mathematics 147], American Mathematical Society, Providence, Rhode Island, 1993, pp. 295–301.

[10] N. Robertson, P.D. Seymour, Graph minors. XIII. The disjoint paths problem, *Journal of Combinatorial Theory, Series B* 63 (1995) 65–110.

[11] A. Schrijver, Disjoint circuits of prescribed homotopies in a graph on a compact surface, *Journal of Combinatorial Theory, Series B* 51 (1991) 127–159.

[12] A. Schrijver, Disjoint homotopic paths and trees in a planar graph, *Discrete & Computational Geometry* 6 (1991) 527–574.

[13] H. Servatius, Automorphisms of graph groups, *Journal of Algebra* 126 (1989) 34–60.

[14] P.D. Seymour, Directed circuits on a torus, *Combinatorica* 11 (1991) 261–273.

[15] M. Sholander, Trees, lattices, and betweenness, *Proceedings of the American Mathematical Society* 3 (1952) 369–381.

[16] M. Sholander, Medians and betweenness, *Proceedings of the American Mathematical Society* 5 (1954) 801–807.

[17] M. Sholander, Medians, lattices and trees, *Proceedings of the American Mathematical Society* 5 (1954) 808–812.

[18] C. Wrathall, The word problem for free partially commutative groups, *Journal of Symbolic Computation* 6 (1988) 99–104.